"CAROL I" NATIONAL DEFENCE UNIVERSITY
Centre for Defence and Security Strategic Studies

P R O C E E D I N G S

INTERNATIONAL SCIENTIFIC CONFERENCE
STRATEGIES XXI
12TH EDITION

THE COMPLEX AND DYNAMIC NATURE OF THE SECURITY ENVIRONMENT

Volume 2

Editors
Stan ANTON
Alexandra SARCINSCHI

November 25-26, 2014
Bucharest - Romania

ISSN 2285-9896
ISSN-L 2285-8318

CONTENTS

SOCIOLOGY AND INTELLIGENCE - LIMITATIONS AND OPPORTUNITIES

Andrei-Marius DIAMESCU
Colonel, PhD, Senior analyst within the Ministry of National Defence.

Abstract*: The article approaches two of the main social investigation paradigms, frequently used in sociological research, and the way in which they can be used in intelligence analysis/production.*

After a critical assessment of the usefulness of the deterministic paradigm in evaluating the domestic/international security environment, in its second half the article focuses on opportunities offered to intelligence analysts by the interactionist perspective on security problems.

The epistemological approach to intelligence, validated by the use of scientific research methodologies, offers intelligence professionals the necessary tools to continuously improve the quality and the objectivity of the products meant for strategic decision makers.

Keywords*: epistemology; sociology; intelligence; determinism; interactionist paradigm; perverse effect.*

Introduction

The society, in any of its social organization forms, is based on social actions and decisions. Both are responsible for the state of the society at any given moment of its existence. As long as decision making and action are not under the pressure of correct interpretations, preferably scientifically validated, but under that of improvisation and empirical options based on *common sense,* the social change will take place arbitrarily, spontaneously, sometimes with an unwanted and uncontrollable dynamics.

This is why, when it comes to the analyses focused on the concept of *national security,* and military security implicitly, the main concern is to find the most efficient methodologies that identify and assess the sources of insecurity, as well as the solutions to diminish their effects.

The state of security can be correctly or incorrectly assessed, and the assessment, not taking into account the optimum situations, can trigger inadequate actions or insufficient responses that do not contribute to reaching the targets, which most frequently, when talking about security, can be vital for the state of the nation as a whole.

This supports the statement according to which military security is affected by the intelligence's ability to carry out assessments and to intervene, in other words - to process information.

Therefore, I believe that the responsibility for accurate information processing, which belongs mostly to intelligence specialists, is often at least as big as that of strategic decision makers (political, military, financial-economic etc.).

Undoubtedly, *intelligence analysts* use various methodologies, each of them with a certain degree of abstractedness and comprehensiveness.

In social sciences, concepts such as *security, justice, peace, equality, freedom etc.* include an entire area of expertise and this is why they cannot be defined in general terms. They require a theoretical analysis to identify their limits of applicability, the contradictions which may appear and the impact of the new trends.

Therefore, *I believe that the similarity between intelligence as a field of study, and sociology is relevant*, as Boudon stated: "all sociologists or nearly all of them have tried to define the object of sociology, which is another way of saying that no one has reached this goal... and no definition has been universally accepted"[1].

1. The limitations of the deterministic paradigm in researching security problems

The explanation focused on *causes* has been and most likely will remain the simplest form of explanation and, hence, the most frequently used. Based on the actual progress of successions, the phrase *"if A (before B), then B"* defines the *deterministic paradigm*.

The first difficulties that stemmed from the hasty causal analysis of the situations people are confronted with led to *logics,* as an attempt to introduce rules which would make possible the use of causal thinking patterns. The delimitations introduced by these types of *rules* have favoured the theoretical analyses which have gradually produced scientific ways of investigating certain phenomena by using the data provided by observation and experiments.

The causal way in which the determination relations can be explained had a large impact on security analysis. Most analysts, at least at first, concluded that the analytic approach should be focused on searching and identifying *laws.*

The interpretation of social existence as governed by regularities, *dominant at the beginnings of sociology*, has gradually caught the attention of researchers. They soon realized that most of them, believing the fields of study to be cognizable by identifying the laws, create various ways of analysis to define the regularities which govern the field under investigation. In other words, the tools of study become objectives that have to be proven, a situation in which the area being studied becomes quite inconsistent.

Sociology and social sciences in general began to produce causal explanations as they developed. However, researchers found in time that more and more social situations cannot be explained through causal determination relations.

Some sociologists, among them Raymond Boudon, even denied that causal analyses would play any part in social investigations: "in all the cases in which sociologists managed to decipher obscure phenomena, they used analyses of the interactionist type; the phenomenon is explained through composing some individual actions whose logic cannot be reduced to stimulus-response or cause-effect patterns (...) the sociological analysis cannot be based on a model which turns individual behaviour into the product of social structures. Attempting to eliminate the freedom of the subject, the sociologist can fall into the trap of reductionist paradigms"[2] .

In fact, causal interpretation is only one of the ways to interpret determinations from the field of security. Analysing it, we can safely say that it can be disputed based on at least three arguments:

- the interactions among various internal structures dealing with national security issues and the interactions between these structures and international organizations are often ignored;
- quite often the process in which internal security organizations take up roles is neglected;
- by ignoring the internal organization and reducing the interactions between them to *variables* determined by causes, the analyst cannot make pertinent judgements.

---

[1] Raymond Boudon, *„La crise de la sociologie",* cf. Mattei Dogan, Robert Pahre, *„Noile ştiinţe sociale - interpenetrarea disciplinilor",* Bucharest, Editura Academiei Române, 1993, p. 114.

[2] Raymond Boudon, *Texte sociologice alese,* Editura Humanitas, Bucharest, 1990, p. 256.

When developing a critique of determinism applied to the field of security, the role of politics in drafting security strategies should not be forgotten. In the real world, politicians are only partially informed and this is why, obviously, they don't fully understand the other participants in the process. Consequently, many factors in the process of establishing the politics have nothing to do directly with security and, nevertheless, they have a considerable influence on the policies proposed in the name of national security. Since politics has a powerful impact on security issues, the process of establishing it makes it impossible to apply a causal analysis pattern in the field of security.

2. Opportunities offered by the interactionist analysis of security issues

The main requirement of this perspective, clearly stated by French sociologist Raymond Boudon in *"Perverse Effects and Social Contradictions",* is to include any fact, phenomenon or social process in the explanation as a result of *individual* actions. By *individual* Boudon means either a human or an organized group which has decision-making power, able to target its own purposes based on well-acknowledged intentions and motivations.

Also, the "perverse effect" concept is introduced*,* an effect defined as the unintended result of individual actions, oriented by intentions. This result can be both wanted and unwanted from the action agent's viewpoint.

Adopting this sociological formula, Boudon states:

- all the macro-social aspects derive from individual actions and their combinations;
- the constraining exterior forces are - in the end - nothing else but the unintended result of a multitude of intended individual actions.

In order to emphasize how useful the Boudon-ian perspective on the interrogation of the social could be when carrying out pertinent security analyses, I found very useful the rough sketch which shows the main highlights of the French sociologist's contribution, drafted by Ioan Aluaş and Traian Rotariu[3]:

a. Boudon's premise is that the *individual agent* is the logical nucleus of the action and this is why any explanation of the facts, phenomena or social processes should take into account, eventually, individual actions. The explanation mentions social factors whose existence is quite doubtful, such as *group conscience, collective will,* concepts used by the communist ideology, yet still present today in political speech.

This premise leads us almost instinctually to the role attributed to states by the definition of international society: "The international society is a group of states (politically independent actors), which form more than a system, as each state's behaviour is a necessary factor taken into account by the others, which have established through dialogue and consensus some common rules and institutions to preserve their relations and to maintain this arrangement"[4].

In the analysis of internal security *individual agents* can be easily recognised as well: institutions, political parties, non-governmental organizations etc.;

b. any individual action has a *purpose.* It can be admitted that most individuals follow objectives that would satisfy their needs and interests (generally with an adaptive purpose), as their rationality allows them to act effectively, choosing the most suitable means for their purposes. This rationality is not absolute or perfect, since in most situations the individual agents do not have all the possible information regarding the context and they cannot predict in a precise manner the consequences of their actions.

---

[3] Ioan Aluaş; Traian Rotariu, prefaţă la *Texte sociologice alese.* Editura Humanitas, Bucharest, 1990, p. 12-14.

[4] [10]Hedley Bull, Adam Wolson, conform Barry Buzan, *Popoarele, Statele şi teama,* Editura Cartier, Chişinău, 2000, p. 173.

Applied in the field of security, this premise offers us a reason for the existence of most instruments, both national and international, all of which aim to prevent and manage insecurity sources. International and domestic institutions which manage external relations are meant to guarantee the international security framework, while *intelligence services provide to decision makers and individual agents the optimum amount of information needed for management;*

c. Individual actions should be understood in the sense that the intelligence analyst, placing himself hypothetically in the agents' situation, should be able to determine their probable course of action.

In Boudon's opinion, understanding the agents' actions does not imply subjectivity, does not require certain abilities, skills or special psychological traits that would allow the analyst to identify himself with *living/reliving* the action.

Moreover, understanding is not focused on a certain individual, which would inevitably imply the taking into consideration of certain personality traits, some data which would be difficult to gauge objectively in the absence of adequate psychological studies. Actually, the understanding is directed to the actor as a representative of a social group. Therefore, *the understanding difficulties, the possibility of erroneously interpreting the actions of agents do not stem from a potential psychological or cultural incompatibility between the intelligence analyst and the subject, they derive only from a potential lack of information regarding the social context of the action, more precisely the structural factors which lead actions into certain directions.* Reconstituting accurately the context in which the action takes place virtually eliminates any subjectivity in understanding the actors' actions;

d. The last in line, yet the most important premise in terms of consequences, is *the logical reconstruction of the studied social fact as a result of individual interactions*.

This reconstruction can be intuitive and immediate, and the social result will easily stem from the multitude of individual actions. In this case, the explanation scheme is reduced to a few sentences which state the options and values attached to them by individuals in the analysed social framework with the conclusion resulting directly from these sentences.

In other cases, the situation can be more complex, and some mathematical methods may be required for the assembly of individual actions. Sometimes the result of individual actions (the actors' actions) is the direct extension of these actions; *at other times, it can lead to a phenomenon or a process that no one was expecting, unwanted for some or all participants in the action.*

At this point in his theory, which I consider to be highly important for the intelligence analysis, the French sociologist introduces the *perverse effect* concept.

Without claiming to be the creator of this concept, which he attributes to philosophers Smith and Rousseau, Boudon defines the perverse effect as follows: "when two individuals (or more), following a certain objective, generate an unexpected state of facts which can be considered unwanted by both or one of them"[5].

Maybe the best example of a perverse effect seen in the case of international security relations was the unprecedented escalation of the arms race generated during the Cold War by the nuclear deterrence theory.

Another perverse effect in my opinion would be what happened in the U.S. prior to the 9/11 terrorist attacks in terms of the intelligence services' activity: *the dissipation of strategic information led to a deficit of integrated interpretation and analysis and implicitly to the decision makers' information deficit.*

In the field of defence we should also mention *the perverse effect of war***,** used by Boudon to illustrate the case in which *individuals* might not reach their objectives even if they use the best means to achieve them: in this case, the escalation of conflict leads to

[5] Raymond Boudon, *Texte sociologice alese,* Editura Humanitas, Bucharest, 2000, p. 159, 165.

considerable losses for the antagonists and ends in incertitude.

Of course, there are many examples of perverse effects, both on a micro-social and a macro-social level. I will just mention a type of perverse effect which Boudon noticed in Merton's "*The Unanticipated Consequences of Purposive Social Action",* regarding *creative prediction*, which I consider worthy of the intelligence analysts' attention, especially when powerful actors are being considered.

According to Merton, predictions sometimes tend to come true because *a prediction can become a social fact once it has been stated*. If a considerable number of people, in comparable situations, share the same beliefs and issue the same predictions, a perverse effect would be born and in this case it would be an effective realization of the aforementioned predictions.

The example which I think best illustrates this theory of creative predictions is the collective belief in the banks' insolvency, which led to the hasty simultaneous withdrawal of money and thus to numerous bankruptcies.

Going back to the question: *What approaches could give intelligence analysts the possibility to correctly interpret the problems in the field of security/insecurity sources and to find efficient ways of intervention?* Raymond Boudon gives us a potential answer*: focusing the analysis on interactions.*

This might be a good thing, because the actions/interactions between the actors involved lead to processes which transcend their intentions, which is why ignoring the consequences derived from these actions and their products is a methodological error which hinders the accurate interpretation of the analysed field.

The interactions are usually caused by pressures induced by necessities, and the need for security is essential for the survival of any organization, including the state and nation.

Also, the interactions imply differences between the actors involved, their synchronization and complementarity.

In interactions, the actors, *the individual agents* as Boudon calls them, become aware of correlation needs determined by the expected results. However, regardless of the expected results, in most cases the interactions produce also derived consequences which can be favourable to the purposes or not.

Because of these reasons, the analyses have to be drafted so they would reveal all the types of consequences derived from interactions, as well as the ways of intervention for the optimization or the elimination of wanted/unwanted effects.

Regardless of the paradigm in use, the diagnoses, and especially the analyses with a constructive ending in the field of security should speak about:

- the functional reasoning of interactions;
- the characteristics of interactions;
- the derived consequences produced by interactions;
- the implications of these consequences for the analysed field/issue;
- the potential sources of dysfunction in providing security (sources of insecurity);
- the possibilities to improve the sources of insecurity.

Even if according to Boudon *"in all the cases in which sociologists managed to decipher obscure phenomena they used interactionist analyses"*, at the moment the reading of some studies in the field of security shows that this method is not the best, nor unanimously accepted.

Conclusions

The common theme for these aspects that I have presented is that in order to approach the issue of security one has to display a comprehensive understanding of the main levels of

the social and its subdomains.

Because of these reasons the solution lies in using an integrative analysis in terms of investigation and methodologies. Of course, giving up on one theory is not enough to carry out pertinent studies in the field of security.

The assessment method that relies on comparison is useful when pinpointing the errors embedded in the chosen interpretative theories and, secondly, when orienting the intelligence analyst to the suitable methodology.

Any study dedicated to security should not ignore the antinomy accepted by epistemology which states that *the social universe is divided between two worlds: an easily accessible, hence suspicious, world and another one that is very opaque, hence rich in meaning.*

Gaston Bachelard remarkably summarized this antinomy stating that *"no science conceals anything"* and encouraged researchers to *"remain extremely vigilant against the superficial representations of common sense"* [6] .

Concretely, the intelligence analyst has to constantly clarify the intentions displayed publicly by the actors involved in the field of security, as well as the goals pursued by them. The analyst has to reveal the dynamics of interests and the way the strategy unfold beyond the apparently noble speeches.

The analyst has to see beyond the reasons given by the actors and to reveal *the motives* or *justifications* which hide the real reasons.

A well-structured analysis is meant to reveal manipulations; an analysis which merely describes security mechanisms, unfortunately quite frequent, fulfils the role of a clerk or that of an explainer, failing to be constructive in any way.

Acknowledgement:

This work was possible with the financial support of the Sectoral Operational Programme for Human Resources Development 2007-2013, co-financed by the European Social Fund, under the project number POSDRU/159/1.5/S/138822 with the title ***"Transnational network of integrated management of intelligent doctoral and postdoctoral research in the fields of Military Science, Security and Intelligence, Public order and National Security – Continuous formation programme for elite researchers - "SmartSPODAS"."***

BIBLIOGRAPHY:

1. ANGHEL, Gheorghe, *Componentele securităţii naţionale a României*, Ed.Societăţii TEMPUS, Bucharest, 1996.
2. BOUDOIN, Jean, *Introducere în sociologia politică*; Ed.Amarcard, Timişoara, 1999
3. BOUDON, Raymond, *Teste sociologice alese*, Ed.Humanitas, Bucharest, 1990
4. BUZAN, Barry, *Popoarele, statele şi teama*, Ed.Cartier, Chişinău, 2000.
5. CULDA, Lucian, *Dimensiunea epostemologică a interogării existenţei sociale a oamenilor*, Ed.LICORNA, Bucharest, 2000.
6. DAVIN, V. Aurel, *Naţiunea, între "starea de securitate" şi "criza politico-militară"*, Ed.Licorna, Bucharest, 2000.
7. DEAC, Aron Liviu; IRIMIA, Ion, *Securitatea României la răscrucea de milenii*, Ed.Academiei de Inalte Studii Militare, Bucharest, 2000.
8. DOGAN, Matei; PAHRE, Robert, *Noile ştiinţe sociale – interpretarea disciplinelor*, Editura Academiei Române, Bucharest, 1993.

[6] Cf. Jean Baudouin, *Introducere în sociologia politică,* Editura *Amarcord,* Timişoara, 1999, p. 19.

9. IACOB, Dumitru; Cismaru Diana-Maria, *Organizaţia inteligentă – 10 teme de managementul organizaţilor*, Ed.comunicare.ro, 2002.
10. POPPER, Karl R., *Logica Cercetării, Ed. Ştiinţifică şi Encioclo*pedică, Bucharest , 1981.
11. *** *Interesul naţional şi politica de securitate*, Institutul Român de Studii Internaţionale, Bucharest, 1995.
12. *** *România în situaţii limită, Ministerul Culturii şi Societatea România Secolului XXI*, Licorna Publishinghouse, Bucharest, 1995.
13. *** *Securitate şi apărare naţională, sesiunea de comunicări ştiinţifice, 26 aprilie 2001*, EdituraAcademiei de Înalte Studii Militare, Bucharest, 2001.
14. *** *Situaţia naţiunilor – surse de insecuritate, Societatea România Secolului XXI*, Licorna Publishinghouse, Bucharest, 1999.

THE IMPACT OF DIGITAL TECHNOLOGIES ON REDEFINING SECURITY

Elena Adelina ANDREI
PhD. student in Intelligence and National Security within "Mihai Viteazul" National Intelligence Academy, Bucharest, Romania.
E-mail address: andrei.adelina@yahoo.com

Alina MÎLCOMETE
PhD. Student in Intelligence and National Security within "Mihai Viteazul" National Intelligence Academy, Bucharest, Romania.
E-mail address: alina.milcomete@yahoo.com

***Abstract**: When we speak about the impact of technology on society and security, in most of the times, are stressed the positive effects of technology and how they facilitate an easier course of life of each individual. The trends of the past five years indicates that a number of small and large institutions around the world have adopted digital technologies in various forms - public, private, hybrid, and this is currently on a slope upward. The digital technologies, such cloud computing, have been associated with a paradigm shift in technology for users, in terms of scalability and resource sharing, while at the same time, this represents a security risk.*

***Keywords:** digital, technology, cloud computing, cloud applications, public cloud, private cloud*

Introduction

In the last ten years, the number of Internet users - one of the most important infrastructure in the 21st century, has increased by 20 times, reaching 1.5 billion in 2008, and the number of servers went up from 22.5 million to 489 million. In this context, the Internet architecture, to which more and more individuals will have access at the global level, will be faced with more complex challenges. Thus, Europe has commited itself to have a coordinating role in exploring new visions of the future of Internet[1].

The first stage in the technological advance consists in the fact that technology will fall below a "critical price": "after this, it will tend, if it is successful, to rise above a critical mass". At one point, many technologies displace another technology, and then finally, a lot of technologies commoditize. Towards the end of their life, they become nearly free[2].

Also, technology is "enabling trust between strangers". Individuals now seem to live in a "global village" where we can mimic the ties that used to happen face to face, but on a scale and in ways that have never been possible before. So what's actually happening is that social networks and real-time technologies are taking us back: "We're bartering, trading, swapping, sharing, but they're being reinvented into dynamic and appealing forms. Now as our possessions dematerialize into the cloud, a blurry line is appearing between what's mine,

[1]European Union, *Digital Agenda for Europe: An Europe 2020 Initiative*, http://ec.europa.eu/digital-agenda, accessed on 11.09.2014.
[2]Chris Anderson, *Technology's long tail*, Ferbuary 2004, http://www.ted.com/talks/chris_anderson_of _wired_on_tech _s_long_tail, accessed on 11.09.2014.

what's yours, and what's ours"[3].

1. Cloud Computing - A Current Trend and a New Business Model

Cloud computing has been a sintagm extensively used by a huge number of businesses in the complex computing industry, but without having a fully understanding of what its benefits are. One of the main reasons of this fact is that the networking infrastructure was still in its infancy and individuals could not understand the full potential of cloud computing, until now. The technology has been „steadily gathering momentum in many of today's industries", with IT's biggest corporations such as, Amazon, Google, Microsoft and Salesforce.com etc. Most of them state that cloud technology aim to be the „the fifth generation of computing".

Industry experts in the field of information technology expected that, in the next decade, the evolution of the Internet will face some main trends, cloud computing being identified as one of them[4].

In this regard, a recent study edited by the "Telecom Trends International" estimates that, by 2015, cloud computing will produce an income of over 45.5 billion dollars. This is why the National Science Foundation (NSF) encourages researchers not only to devise better ways of representing users and applications in a cloud computing infrastructure, but also to take into account other tools to measure the performance of cloud-based services. It is expected that the Internet will experience a new direction by participating in the creation of a new world in which individuals will live in a 3D transparent media cloud, surrounded by intelligent and intuitive interfaces embedded in everyday objects[5].

Cloud computing can be seen as "a new approach to IT", of its scalability and of the implementation of the immense capabilities that offer new storage and virtualization technologies. The reducing of the cost implementation, operation and efficiency are the words that mobilize resources, companies, developers to answer to all the challenges of this new business model. Based on existing infrastructure that can be built for the benefit of IT services at any time, millions of users have a strong argument for both large vendors and a number of key suppliers of products and services to mobilize the implementation of cloud computing and virtualization[6].

Also, according to Cisco Vice President, Lew Tucker, cloud computing comes just in time to support the technological changes that undergo in the present. The Cisco strategy of occupying a large part of the market is based on three pillars: to be an infrastructure provider for those who are building cloud services, to provide solutions for implementing cloud services (by EMC, NetApp, VMware, etc.) and to contribute to accelerate the use of these services by providing tools to access the cloud.

The third part of the study "Cisco Connected World Report"[7] reveals that among the 13 participating countries worldwide, 52% of IT professionals said they use or plan to use applications such cloud, as these applications are being used more widely in Brazil (70%), China (69%) and India (76%).

---

[3] *Ibid*.

[4] Carolyn Duffy Marsan, *10 Ways the Internet Will Change in 2010*, in PCWorld, 4 January 2010, http://www.pcworld.com/article/185768/10_ways_the_internet_will_change_in_2010.html, accessed on 11.09.2014.

[5] Valentin Petru Măzăreanu, *Tehnologii mobile: de la conexiune fără fir la internetul lucrurilor*, http://www.scribd.com/doc/22053711/Tehnologii-Mobile-de-La-Conexiune-Fara-Fir-La-Internetul-Lucrurilor, accessed on 11.09.2014.

[6] Dan Falconer, *Desktop, Server, Cloud – Your Quest for Simple Management*, 2011, http://www.idg.ro/cloud, accessed on 11.09.2014.

[7] Cisco, *Connected World Report. Part 3. Data Center*, http://www.slideshare.net/Cisco/cisco-connected-world-report-part3?from=ss_embed, accessed on 11.09.2014.

Across the world, respondents highlighted the following priorities for the coming years: improve agility and speed in implementing business applications (33%), increase the ability to better manage resources in order to match demand (31%), increase the resilience center data (19%) and reduction of costs of energy (17%).

Within the 13 countries surveyed, only an average of 18% of respondents use this type of applications today, while 34% plan to use them.

The top users of cloud applications by country is as follows: Brazil (27%), Germany (27%), India (26%), USA (23%) and Mexico (22%) - topped on the list of countries that are using these applications with a higher proportion than average of 18% of all countries.

2. Types of Cloud Applications. The Impact on National Security and Intelligence Community

A majority (88%) of respondents of the survey[8] predict that IT specialists will store some of the data structures and applications of their companies in public or private cloud over the next three years. [9]

One in three IT professionals claim that more than half of their corporate data and applications will be on private cloud applications over the next three years. Adoption of private cloud applications is expected to be higher in Mexico (71%), Brazil (53%) and the USA (46%).

Among respondents of the same study[10] who said they use public cloud applications, 34% were planning to use them in the next year, 44% in the next two years and 21% were planning to use them in the next 2-3 years[11].

Regarding the types of Cloud Computing, there are forms of public, hybrid and private cloud. Public Cloud is the classic form of cloud computing where users can access applications or services through the web browser. Also, the hybrid Cloud is a hybrid environment, where virtualized and physical servers require routers and enable a safer accessing to users.

In what private Cloud regards, as the name suggests, it refers to a private environment, such as, the governmental one, which can be accessed only by users who have access to that network[12].

One of the major benefits consists in the fact that the emerging technology allows companies to match the technical multinationals resources. According to specialists, the most advanced technologies in the world are locally available and the cost of using the service is very low. Companies that are 3 or 3000 employees can use in cloud services and the price will be directly proportional to use on the pay-as-you-go.

Cloud services integrators such as Appnor are the missing link for widespread cloud adoption because they have the necessary expertise to assist companies migration to these solutions.

Also, Cloud solutions eliminate several categories of costs: costs for servers, software licenses, hosting, collocation, maintenance, technical ultraspecialized upgrades of all kinds, annual subscriptions, etc.

---

[8] *Ibid*.
[9] *Ibid*.
[10] *Ibid*.
[11] *Ibid.*
[12] Lupu Cosmin, *Cloud Computing – Everything You Want to Know*, 15.02.2010, http://www.slideshare.net/lupucosmin/cloud-computing-everything-you-whant-to-know, accessed on 11.09.2014.

According to a HP study[13], "in an unpredictable economic environment in which IT infrastructure feel pressure to support a higher volume of services and applications with lower costs, cloud computing solutions offer affordable delivery model and ensures companies with more flexibility to conduct daily business". It shows that managers of companies around the world believes that, by 2015, 18% of their IT services will be delivered through public cloud solutions and 28% through a private cloud solution. Thus, almost half of business services serving companies will be moved "in the cloud", an important change compared to traditional IT structures that currently exist.[14].

In Romania, this industry is at the beginning and consider Appnor the first integrator of cloud solutions. According to experts, a large barrier is the local support that international providers of cloud services do not grant, requiring a process of educating the market; companies do not yet know why individuals should prefer the cloud and use old solutions of inertia, bearing the costs.

Through the information technology provided, cloud computing enlarges to meet the individuals of the Intelligence Community's needs and narrows when the demand diminishes. It redefines national security system by enabling more swiftness in support of operational missions and widens access to computational power, through reducing costs.

In their adoption of cloud computing, the national security organizations have to be liable of enhancing new roles and functions and revise their processes and policies.

Within the Intelligence community, the cloud computing's impact uniquely addresses critical defence and intelligence mission need by uncover data and applying in to the mission.

The cloud computing model can significantly help national security agencies grappling with the need to provide highly reliable, innovative services quickly, despite resource constraints. Commercial service providers are expanding their available cloud offerings to include the entire traditional IT stack of hardware and software infrastructure, middleware platforms, application system components, software services, and turnkey applications.

The enactment of a cloud computing solution may add security benefits, but only with planning, work and engineering focused on security.

Taking into consideration that in cloud models, act more directorate points than in traditional date centers, new technical paths turn to introduce new attack vectors. In this case, there are current fields where specific controls demand to be enforced. Refined detection systems may be convenient, but the competitor can be ahead of the trajectory that controls the response time for security events and breaches.

By and large, advanced risk managements, with the new trust borderline would drive specific security controls for supervisor layers.

Cloud computing has resulted in greater agility, cost savings and efficiency for many national security organizations, but also increases the vulnerability of crucial data and may threaten cyber-security. As cloud computing pursues to emerge, the need for the protection of internal and external networks will expand exponentially for companies, national security individuals and end users. Although many security threats are predictable and preventable, national security organizations and companies need to be more diligent in protecting data stored on their networks from the everyday behavior of company employees.

---

[13]Hewlett Packard, *HP Hybrid Delivery*, 2011, http://www.hp.com/hpinfo/newsroom/press_kits/2011/EBcloudcomputing2011/HybridDeliveryFactSheet12011.pdf.

Bârzoi Vali, *Studiu HP: Până în 2015 aproape jumătate din serviciile IT vor fi livrate prin soluții de cloud computing,* http://www.businesscover.ro/01-12-2010-studiu-hp-pana-in-2015-aproape-jumatate-din-serviciile-it-vor-fi-livrate-prin-solutii-de-cloud-computing, accessed on 11.09.2014.

[14]*Ibid*.

3. Cloud Computing Trends: 2014 State of the Cloud Survey

In the third annual State of the Cloud Survey, conducted in February 2014, RightScale asked 1,068 technical professionals across organizations about their adoption of cloud computing. Twenty-four percent of respondents were from big dimensions enterprises, with more than 1,000 employees[15].

According to the Survey, 94 percent of surveyed organizations are "running applications or experimenting with infrastructure-as-a-service" and 87 percent of them "are using public cloud". Even though the adoption of cloud is significant, only 29 percent use only the public cloud and 7 percent use only the private cloud; on the other hand, 58 percent use both public and private[16].

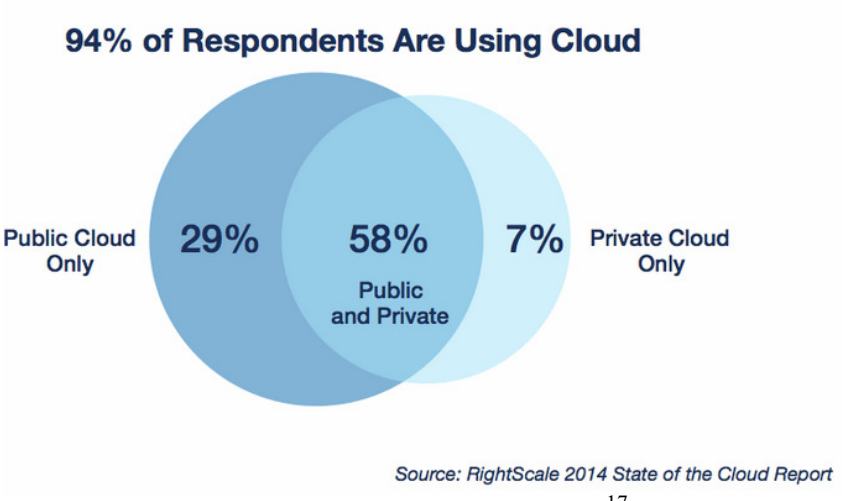


Figure no. 1. Cloud Adoption[17]

The 2014 survey "echoes a key finding of the 2013 Report", "the Cloud maturity matters". Organizations exposed cloud more broadly, they recognize the added value and the challenges of adopting cloud. Organizations indicate that the top benefits that they have already realized are greater scalability, faster access to infrastructure, higher availability, and faster time to market for applications[18].

[15] RightScale, *Cloud Computing Trends: 2014 State of the Cloud Survey*, February 2014, http://www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2014-state-cloud-survey, accessed on 11.09.2014
[16] *Ibid.*
[17] *Ibid.*
[18] *Ibid.*

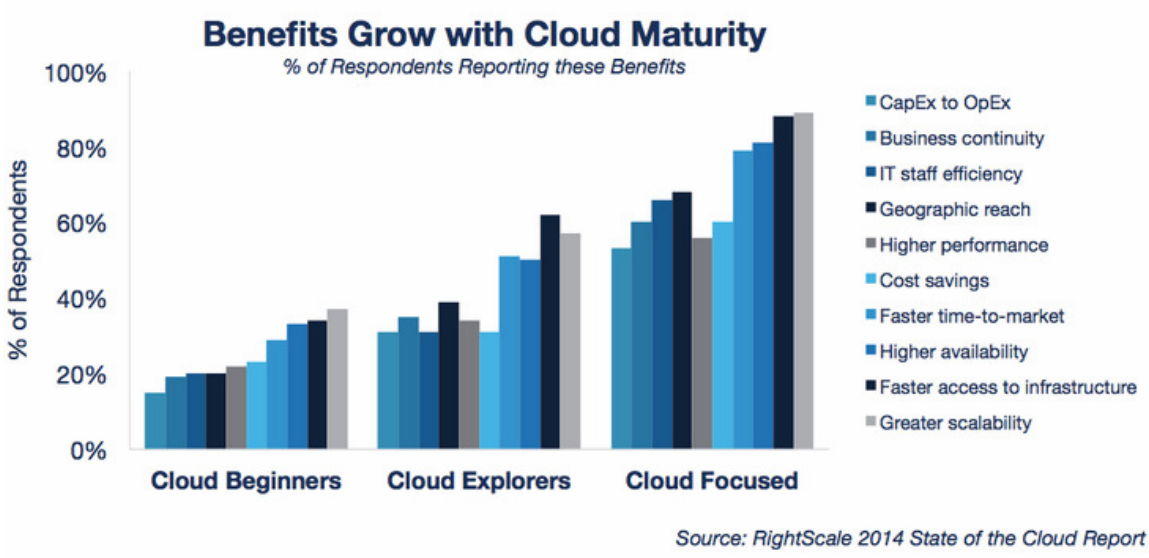


Figure no. 2. Benefits Grow with Cloud Maturity[19]

While the benefits of the cloud change with experience, the challenges of cloud show an abrupt decrease in the same time institutions acquire expertise with cloud. In this context, security continue to be the most-frequently mentioned challenge through Cloud Beginners (31 percent), but minifies to "the fifth most cited (13 percent) among Cloud Focused organizations". As institutions turn to be more experienced in cloud security options and best practices, "the less of a concern cloud security becomes". Concerns about cloud security "declined in 2014 among both Cloud Beginners and Cloud Focused respondents"[20].

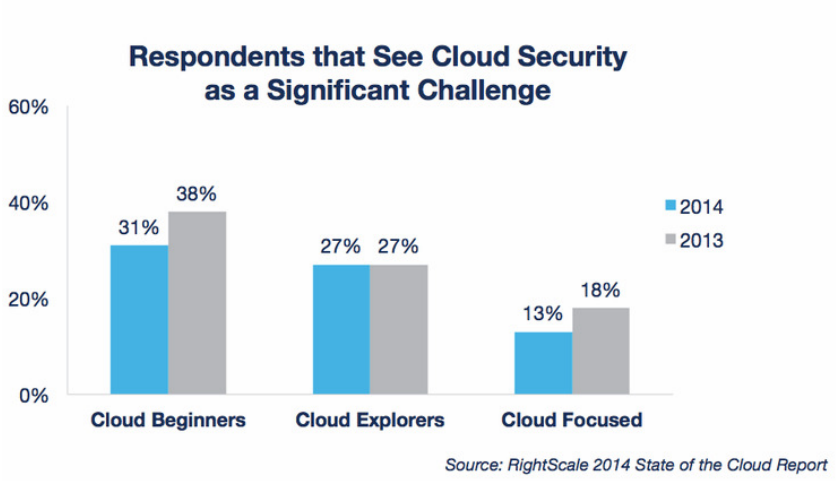


Figure no. 3. Cloud Security – a Significant Challenge[21]

In the context of the challenge appearance of cloud security diminishes with cloud maturity, other quests require attention in Cloud Focused organizations. Security and compliance preserve to be an issue for 31 and 30 percent of Cloud Beginners users, representing the most extended challenges. Also, compliance occupies the first place concerning through Cloud Focused Organizations.

In addition, cost and performance "occupy the second and third slots as organizations

[19] *Ibid.*
[20] *Ibid.*
[21] *Ibid.*

need to focus ongoing attention on these issues" [22].

Top 5 Challenges Change with Cloud Maturity

Place	Cloud Beginners	Cloud Focused
#1	**Security (31%)**	Compliance (18%)
#2	Compliance (30%)	Cost (17%)
#3	Managing multiple cloud services (28%)	Performance (15%)
#4	Integration to internal systems (28%)	Managing multiple cloud services (13%)
#5	Governance/Control (26%)	**Security (13%)**

Source: RightScale 2014 State of the Cloud Report

Figure no. 4. Top Challenges Change with Cloud Security[23]

Conclusions

Cloud Computing is one of the technologies that already make the difference in this reference. There are still plenty of confusions in the industry, especially among users who asks about what cloud computing is, how it can be used and the problems that may arise in migrating between business processes. Finally, there remains the problem of data security, especially for the public cloud.

The 2014 State of the Cloud Survey indicates that the time for cloud adoption has arrived. The vast majority of institutions have already "embarked on a cloud journey" that will make IT a critical component of corporate growth and profits.

Also, IT organizations are rapidly moving toward a world where they can offer a portfolio of cloud services, both public and private, to meet the diverse requirements of their applications. Organizations are "already seeing significant benefits from their use of cloud, and the barriers to adoption are rapidly disappearing. As a result, each step companies take in their cloud journey delivers increasing value".

Acknowledgement:

This paper is made and published under the aegis of the Research Institute for Quality of Life, Romanian Academy as a part of programme co-funded by the European Union within the Operational Sectorial Programme for Human Resources Development through the project for Pluri and interdisciplinary in doctoral and post-doctoral programmes Project Code: POSDRU/159/1.5/S/141086

Sectoral Operational Programme Human Resources Development 2007-2013.

Project title: Pluri and interdisciplinary in doctoral and post-doctoral programmes

Editor of material:

Date of publication:

The contents of this material do not necessarily represent the official position of the European Union or the Romanian Government.

[22] *Ibid.*

[23] *Ibid.*

BIBLIOGRAPHY:

1. ANDERSON Chris, *Technology's long tail*, Ferbuary 2004, http://www.ted.com/talks/chris_anderson_of_wired_on_tech_s_long_tail.
2. BÂRZOI Vali, *Studiu HP: Până în 2015 aproape jumătate din serviciile IT vor fi livrate prin soluţii de cloud computing,* http://www.businesscover.ro/01-12-2010-studiu-hp-pana-in-2015-aproape-jumatate-din-serviciile-it-vor-fi-livrate-prin-solutii-de-cloud-computing.
3. FALCONER, Dan, *Desktop, Server, Cloud – Your Quest for Simple Management*, 2011, http://www.idg.ro/cloud.
4. LUPU, Cosmin, *Cloud Computing – Everything You Want to Know*, 15.02.2010, http://www.slideshare.net/lupucosmin/cloud-computing-everything-you-whant-to-know.
5. MARSAN, Carolyn Duffy, *10 Ways the Internet Will Change in 2010*, in PCWorld, 4 January 2010, http://www.pcworld.com/article/185768/10_ways_the_internet_will_change_in_2010.html.
6. MĂZĂREANU, Valentin Petru, *Tehnologii mobile: de la conexiune fără fir la internetul lucrurilor*, http://www.scribd.com/doc/22053711/Tehnologii-Mobile-de-La-Conexiune-Fara-Fir-La-Internetul-Lucrurilor.
7. ***, CISCO, *Connected World Report. Part 3. Data Center*, http://www.slideshare.net/Cisco/cisco-connected-world-report-part3?from=ss_embed.
8. ***, European Union, *Digital Agenda for Europe: An Europe 2020 Initiative*, http://ec.europa.eu/digital-agenda.
9. ***, Hewlett Packard, *HP Hybrid Delivery*, 2011, http://www.hp.com/hpinfo/newsroom/press_kits/2011/EBcloudcomputing2011/HybridDeliveryFactSheet12011.pdf.
10. ***, RightScale, *Cloud Computing Trends: 2014 State of the Cloud Survey*, February 2014, http://www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2014-state-cloud-survey.

REDEFINING INTELLIGENCE THROUGH SOCIAL MEDIA

Raluca LUŢAI
Student at Babeş-Bolyai University, Faculty of History and Philosophy,
Cluj-Napoca, Romania.
E-mail address: raluca_lutai@yahoo.com.

Abstract*: Social media is the most important part of the twenty-first century technological revolution. Because of its impact the ordinary individual's online activities are changing in a way that has a serious impact in the everyday life.*

Social Media is now available for everyone thanks to the development of Web 2.0 and User Generate Content which led to the creation of this sharing environment. Whether the collaborative projects as Wikipedia, social networks like Facebook, blogs and microblogs like Twitter, all forms of social media transforms the user into a producer and consumer of information.

This metamorphosis creates a context in which the intelligence communities are facing some changes. Based on this reasoning, the present work aims to analyze, after a brief conceptualization of the social media phenomenon, the most important changes that the intelligence communities encounter in a social media. To exemplify one of changes in the intelligence community we will briefly review the Romanian Intelligence Service Facebook page.

Keywords*: Social Media, Intelligence, intelligence communities, Romanian Intelligence Service.*

Introduction

The 21st century is without any doubt the speed century. The world flattens, human relations are experiencing a new stage in their development and people's perceptions of reality and the world are changing. The world in the 21st century is a place where communication is a crucial mechanism exploited at maximum by all individuals.

Social Media is today one of the main drivers of this process. Developed under the impact of globalization and accelerating technological developments, the changes that this new form of interaction produces are profound and visible in many aspects of everyday society. Social Media allows individuals to form groups and virtual communities, enabling members to seek and maintain direct connections, to communicate and exchange information, ideas and beliefs. With a simple click the whole world can find out where you are, the work you carry on, the things you like or dislike and the people that surround you.

When society develops new forms and methods of communication, such as social media, public institutions including the intelligence community must be able to adapt to these changes. Intelligence communities worldwide must continually and dynamically reinvent themselves and take into account all the technological changes that are recorded. In this context, the effects that social media address to the intelligence sector are obvious and have several implications that must be considered.

After a brief introduction of the concept of social media and its defining elements, this paper will address the changes that occur in the intelligence sector under the impact of social media.

1. The radiography of a concept: Social Media

Nowadays technology's main purpose is connecting individuals, individuals for whom the Internet connection is no longer a luxury but a necessity. According to a study made by McKinsey Global Institute, in July of 2012, around 1.5 million individuals were using social media[1].

Social Media is a term used to describe various extruded virtual world technologies that are used to connect people in different forms of communication and information exchange[2]. While the term "social media" is a relatively new idea underlying it is not. For many decades, man has used the technology provided by computers to establish links with others, to undertake a process of exchanging information and ideas or to work on various projects. While the technology has changed, the reasoning behind c remained the same. Representing a different form of newspaper or TV show, the evolved variant of traditional communication, Social Media is defined by how is used and the technology that allows us to use it. Given the multitude of issues that characterize the concept and the speed with which changes and progresses in this field are recorded, the definition of this concept is still unclear and can take many different forms. One thing that is quite clear is that today, social media is the biggest change that technology has encountered in the last decade[3].

Social media, by its characteristic elements and the possibilities it provides, came to reflect every facet of modern man social life. This would not be possible if the technology had not evolved as it has evolved today. The concept of Web 2.0 and User Generated Content (UGS) are the main concepts that have made possible the existence of social media.

The concept of Web 2.0 was coined in 2005 to describe a way to produce some software. Today the concept is quite extensive and complex and translates as a technology platform whose content is constantly modified in a collaborative form[4]. Web 2.0 is not a form of advanced internet as will say, is the idea of a combined effort made by several people oriented in a certain direction. The second concept, the User Generated Content is the one that allows the existence of social networks. UGS concept occurred in around 2005 and refers to the media made public by users. Thanks to Web 2.0 and the fact that users are now more open than ever in terms of sharing on the internet information of any kind, made possible the development of several types of social media. The main types are:

- *Collaborative projects*. The most successful example of a collaborative project, which speaks for itself, is Wikipedia. Wikipedia and sites like this, assume that the combined effort of many users may have a more positive outcome for the Internet user.
- *Blogs*. Blogs are a simple way that everyone can become a citizen of the digital world. Taking different forms, focusing on various topics, blogs are the most common form of social media.
- *Content Communities*. YouTube and Flickr are two of the most successful examples of this form of social media. The main purpose of these community sites is to share media content: whether is simple photos or it video material.
- *Social networking*. Social networks are those websites that allow individuals and groups to form "virtual societies"[5] thus building a public or semi-public virtual system. Also, a social network enables its members to create direct connections and relationships with other

[1] Michael Cross, *Social Media Security-Leveraging Social Networking While Mitigating th Risks*,Elsevier,2014, p.7.
[2] *Ibidem*, p. 8.
[3]Meredith Rob, Peter O Donnell, ”A framework for understanding the role of social media in buisiness intelligence systems” in *JDS,* 2011,p.3.
[4] Andreas Kaplan, *Users of the world, unite!-The challenges and oportunities of social media,*Kelly School of Buisiness.p. 3.
[5] Tudor Sălduceanu, Florenţa Toader, *Bloguri, Facebook si Politica*, Ed. Tritonic, Bucureşti, 2009, pp.17-18.

users within the system. Nature and objectives of these connections may differ from one site to another but what makes this phenomenon so special is that social networks not only allows the users to meet new people and interact with them freely and unconditionally, but that it allows free access to other individuals social network. Thus, through a snowball phenomenon, a personal social network can tremendous evolve.

Social networks are a unique space for manifestation. They offer various possibilities of communication and expression and a true social phenomenon with implications in areas such as marketing or politics. The most successful example of a social network is Facebook, a network created to connect people around the world.

The most important feature of this system is "sharing capabilities"[6]. This element of exchange information, beliefs, ideas and visions can be seen as the new way of global activism. Designed to help personal development, development thinking and to streamline the creation of a minimal baggage of knowledge in various fields, sharing has come to reach a unsuspected goal. Living in a world still active in the desire for affirmation, this kind of sharing is used to manipulate or rather to multiply an idea among many other "cyber citizens".

- *Virtual word*s. Virtual worlds, (be they in the form of strategy games, or as miming real world) are operating platforms based on the interactions between different avatars. They are the most advanced form of social media so far. The best known examples of virtual worlds are Second Life and World of Warcraft.

Different types of social media transform the individual from a consumer of information in a generator of information and under this situation the intelligence services around the world are facing major changes.

2. The Intelligence Services in the Social Media Era

"We are at the Beginning of a new era of smart nations, clever continents (...) in which all humans have access to all information in all languages, all the time," [7] said Robert Steele, the American officer who first emphasized the importance of open sources for the intelligence sector. Following this reasoning, we can say that all aspects that define the postmodern individual life are *smart*: if the states where they live are *smart nations* which are guiding their work in the international arena based on *smart power* is more than obvious that the intelligence communities need to make *smart intelligence*[8].

Social Media provides the capabilities and the opportunities to transform intelligence services in smart intelligence services.

After a review of the literature that treats the relationship between social media and intelligence services we can say that the changes that social media brings to the intelligence communities can be divided into three categories: (a) changes to the intelligence process, (b) technological changes and (c) image changes.

If information is power, then the real time flow of data and information circulating in social media is very important for the intelligence community. Social Media transforms the flat information environment into a more fluid and more dynamic one and offers ordinary individuals their own mouthpiece. An example highlighting the importance of the information circulating in social media is given by the tragic event that took place in Norway in 2011. In 2011 extremist Andres Brevik, who managed to kill no more than 77 people in its attack,

---

[6] Alexandru-Brăduţ Ulmanu, *Cartea feţelor. Revoluţia Facebook în spaţiul social*, Ed. Humanitas, Bucharest, 2011, p.172.

[7] Robert D. Steele, "Human Intelligence: all humans, all minds, all the time," în *Strategic Studies,* mai 2010, p.5.

[8] The concept of *smart intelligence* refers to information generated by data-mining on the web and via social platforms and is defined by the work of Kenneth C. Werbin "Spookipedia: intelligence, social media and biopolitics" în *Media Culture Society,* Sage Publications, 33:1254.

posted his manifesto online 90 minutes before starting the tragic attack. If intelligence services would be able to read this manifest and understand the threat they had to face, then maybe the event would have been prevented.

The importance of social media for intelligence in terms of source of great information that provides is linked to the events that have troubled London streets in the same year. The final Police report prepared after the events of 2011 highlighted the inability of the intelligence community to collect, monitor and analyze dates from social media[9].

Analyst standing and exploiting the social media will face many dilemmas. Analyst Anthony Olcott believes that the information in social media have five qualities that affect the whole intelligence process. The first feature is related to the large volume of information available in social media. When he searches for data and information in a social media environment, the analyst will have to distinguish "the noise from the sound". Another important aspect in this sense is the rapidity with which it has to operate with the information, and the problem of finding out the direction from where the information comes. If the old architecture of the intelligence process was oriented in an up-down direction, under the impact of social media the information "flows" either chaotic or in bottom-up direction. In these circumstances the information becomes more difficult to identify and validate[10].Mutations that social media produces at the intelligence process level can also be visible in the INT spectrum used by the intelligence communities. The emergence and development of social media has led to development of Social Media Intelligence, a type of intelligence that focuses on the collection and analysis of information available in social media.

In the context in which the information travels in real time, by analyzing social media the intelligence cycle is accelerated and this situation determines the beneficiaries to take the most reliable measures in short time. Response time is compressed and this causes changes in the intelligence officer's activity. The famous James Bond is overthrown by a "spy" that can search information and preserve a safety and secure world just sitting in front of a computer.

The technological changes that the intelligence community must take in consideration while using social media are related to the tools and programs that the services are using in the process of collecting and analyzing dates and information from social media. Intelligence community must provide the necessary elements to assist the analyst in analyzing the sound and not the noise and to allow him to structure the too chaotic information that comes from social media. In this situation, the intelligence services should be aware of all technological developments which may find utility in their work.

Another important aspect in the relation between social media and the intelligence community is related to the fact that the intelligence services see social media as a perfect mean of communication between them and the citizens they serve and between them and other information services.

Social networks like Facebook and microblogs such as Twitter are already enjoying the official presence of intelligence services. Through these networks, the intelligence services are provided with a "microphone" for announcing the most important events that concern them or the latest national security news. Facebook users can interact with the service and this contributes to enhancing the transparency and accountability of these institutions. Through social media, intelligence services will be obliged to be closer and more accountable in front of their citizens.

---

[9]Nicky Antonius, Rich L., " Discovering collection and analysis techniques for social media to improve public safety" in *The international technoloqy management review*, vol.3, no.1, 2012.p.1.

[10]Jeremiah Burgess**,** *The who, what and how of social media explitation for a combatant commander,* Naval War College, 2013.pp.19-21.

Romanian Intelligence Service and Social Media

Romanian Intelligence Service decided to launch an official page on Facebook, the most popular social network, in May 2013.

The idea behind this action comes from judgments concerning the desire to bring the service closer to the citizens which are using this social network. This idea is outlined in the description section- according to the description, " the page allows the service to undertake a directly without intermediaries dialogue with the citizens."[11] The same section offers the institution contact information and a list whit the milestones of the Romanian Intelligence Service since its foundation. These life events refers to the establishment of the service (26 March 1990) laws by which it operates and the directors who have led it in the past 24 years.

Photos made available by the administrators of the page represent a radiography of the most important events that occur in the institution or at the National Intelligence Academy Mihai Viteazul. Whether are the photos from some exhibitions, conferences that they organized, competitions at which the service attended, various activities they conducted as: event related to the educational program Şcoala Altfel, book launches, information on the National Academy admission or graduation information, the uploaded photos are a great opportunity for the ordinary citizens to be aware of some of the activities that they carry this institution.

Through the statuses that are posted, the Romanian Intelligence Service announces some of the successes they have in the fight against corruption, the support they provide to other authorities dismantle criminal organizations, some aspects in preventing and combating terrorism and cyber activities- fields in which they are the central national authority. To these are added press interviews with top leaders of the service. By presenting these events Romanian Intelligence Service seems a more efficient and transparent service closer to citizens. Through these posts, citizens can comment and engage in direct dialogue with the service.

The attention the service s page enjoys is demonstrated by the 6852 likes (13/09/2014) they gathered since the lunch and by the likes and the comments that appear whenever administrators post something.

Considering these aspects and this brief analysis of the page, we can say that the Romanian Intelligence Service understands the power that social media has and chooses to approach the citizen through the network capabilities offered by Facebook. The Facebook page of the service demonstrates how an institution that deals in most of the time with secret issues can be transparent and accountable in its relationship with his servant. The Romanian Intelligence Service Facebook page the paradigm shift and the evident changes that Social Media produces in the intelligence community, at least in terms of image and communication with the citizen.

Besides the aspect related to the presence of intelligence services in social media for their citizens, social media can be a perfect environment for communication within the intelligence community.

Social platforms can be used in strengthening cooperation and shared experience and good practices between various information services that can lead to improving quality of their work. An example is A-Space (Analytic Space) a social media platform created to be a collaborative framework for all intelligence services of the American intelligence community. The platform provides a venue for all American analysts. A-Space is a place where are discussed aspects related to analysis and processing, use of several tools, software, is a great place to here the news in this field and exchange of ideas and good practices on specific

[11] Romanian Intelligence Service Facebook page, available at https://www.facebook.com/sri.oficial/info, accesed in 13.09.2014.

topics. The usefulness and importance of this area was noted by the civil famous Time Magazine which awarded A-Space platform a place in the top 50 inventions of 2008[12]. Another example of a collaborative project site in the intelligence sector is represented by Intellpedia.

Social media produces noticeable changes and evolutions in the intelligence community. Whether on how communities use this information environment as a space for the collection, analysis, dissemination of information, as raw material or as a mean of communication between them and the citizens and between the various intelligence services, advantages and disadvantages of social media should be integrated as a natural course of development and improvement for the intelligence sector. Impact management of this new form of communication should be as effective as possible.

Conclusions

Social media is the one of the most important part of the technological revolution that the new century recorded. Mutations caused by it can turn the online environment in a place for communications, expression and activism.

The technological progress led to the development of concepts like Web 2.0 and User Generated Content that contributed to the emergence of social media. Social Media is the generic term used to describe various technologies that allow the virtual interconnection of online users through various forms of communication and information exchange. Whether the collaborative projects as Wikipedia, social networks like Facebook, blogs and microblogs like Twitter, all forms of social media transforms the user into a producer and consumer of information.

Given that producers and consumers of information suffers several metamorphoses, the intelligence services whose raw material is the information will have to undergo changes and adjustments. The metamorphoses that occur in the intelligence services in social media are divided into three categories: technological changes, intelligence process changes and image changes.

Intelligence communities around the world will have to adapt their logistics and programs used in the analysis of the social media trends that are recorded. Also, the large amount of information available in social media will change the planning, collection and analysis. Beyond these issues, the intelligence community will use social media as a space of communication between them and the citizens and between them and other information services.

The main vector of the changes that intelligence services are facing is the internet. Online environment transforms not only how individuals interact between them but also how intelligence relates to these changes. Based upon the globalization process and the technological and informational progresses the paradigms that dominated intelligence services around the world are changing. The end of the Cold War opened a new era in the intelligence community in which social media has an important spot.

BIBLIOGRAPHY:

1. ANTONIUS, Nicky, RICH L., “Discovering collection and analysis techniques for social media to improve public safety” in *The international technology management review*, vol.3, no.1, 2012.

[12] Kenneth C. Werbin, *op.cit,*p.4.

2. BURGESS, Jeremiah, *The who, what and how of social media exploitation for a combatant commander,* Naval War College, 2013.
3. CROSS, Michael, *Social Media Security-Leveraging Social Networking While Mitigating the Risks*, Elsevier, 2014.
4. KAPLAN, Andreas, *Users of the world, unite!-The challenges and oportunities of social media,* Kelly School of Buisiness.
5. ROB, Meredith, O DONNELL, Peter, "A framework for understanding the role of social media in business intelligence systems" in *JDS,* 2011.
6. SĂLDUCEANU, Tudor, Toader Florenţa, *Bloguri, Facebook si Politica*, Ed. Tritonic, Bucureşti, 2009.
7. ULMANU, Alexandru-Brăduţ, *Cartea feţelor. Revoluţia Facebook în spaţiul social*, Ed. Humanitas, Bucureşti, 2011.
8. STEELE, Robert D, "Human Intelligence: all humans, all minds, all the time," in *Strategic Studies,* mai 2010.
9. WERBIN, Kenneth C. "Spookipedia: intelligence, social media and biopolitics" in *Media Culture Society,* Sage Publications, 33:1254.
10. Romanian Intelligence Service Facebook page, available at https://www.facebook.com/sri.oficial/info.

OSINT IN THE GLOBALIZATION OF THE ACCESS TO INFORMATION

Teodora-Maria DAGHIE
PhD candidate, University of Bucharest.
E-mail address: daghie.teodora-maria@fspub.unibuc.ro

The intelligence function can reform and adapt
to all three shapers of global, postmodern, risk society or react
to maintain the status quo and become irrelevant in the process[1]

Abstract*: The Internet can be considered an indispensable source of information. The data obtained from the Web is used in education, business, entertainment, recreation, medicine, etc. Cyberspace became the scene of a network of espionage and for the activity of various intelligence agencies and special services running on government, business, and crime. Why is this happening?*

This paper aims to further investigate the intelligence making process and to assert the role played by open sources in the digital world. We believe that they should receive cautionary attention as the amount of data to be analyzed is often too high, and this could lead to intelligence gaps – missing important pieces in the analysis.

The search for information using open source is taken by many civil and military structures working within the field of intelligence and industrial espionage. Positive aspects of the collection of information through open sources are obvious: there is no risk of the failure of the agent and, therefore, damage to his reputation. Such an approach, in addition, allows to save money, do not need to spend money to steal information, sometimes legally.

When solving such problems 80% of the workload is occupied with collection, the remaining 20% - dealing with processing and analysis of the data collected. The study of techniques of business intelligence held special seminars and workshops, which, if desired, can be found on the web. We aim to design a mechanism to further simplify the transformation of open source information into intelligence.

Keywords: *cyberspace, open source intelligence, globalization, challenges.*

Introduction

The human history is shaped by the constant battle of human beings to understand the scenarios in which it develops. The man to achieve this goal has used information timely as a tool to determine the failure or victory on those elements that he wants to conquer. Furthermore, the knowledge of its environment has been one of the factors that have made possible to identify the best areas for development or obtain military victory over their opponents.

Much emphasis is put on information publicly available, this making over 80 percent of the total amount of data collected. However, the importance of data collected from classified sources turns upside down the statistics, making 80% of the most valuable information collected from classified sources. Discover this hidden treasure in the alphabet

[1] Stevyn GIBSON, "Open source intelligence", *The RUSI Journal* 149, no. 1 (February 2004): 16-22, accessed August 24, 2014, http://dx.doi.org/10.1080/03071840408522977.

soup of the overall hyper information is the work of analysts: detecting the relevant points, formulate hypotheses, connect the dots and make a story that enables a new way to understand processes taking place before our eyes.

Until recently, the state monopolized the intelligence systems and methodologies. Today the development of the internationalization processes of both companies and NGOs and the emergence of a lot of public information easily accessible through the Internet has changed the rules. The analysis of public information has become the basis in the global projection of all kinds of economic and social initiatives.

Monitoring open sources allows you not only to preview the object of research and industry, but also to get a more detailed form of the working hypothesis. Note that the monitoring of open sources (newspapers, magazines, etc.) allows you not only to preview the object of research and industry, but allows you to form more detailed working hypotheses (probabilistic assumptions regarding the nature and ways of solving existing problems).

Desk research helps to get an overall picture of the situation, and the study of open sources; surveys help to obtain more information about the situation. Since media, monitoring covers all the problems in general leaving white spots, namely development of the questionnaire is to minimize any gaps.

Monitoring open sources is indispensable for collection of statistical information to justify the sampling procedures, verification and interpretation of the information obtained through field methods, and assessment conducted for marketing purposes.

Preparation of the questionnaire with the hypothesis generated and collected information from the media gives you the opportunity to better the final profile.

Thus, the final profile formed on this basis in the monitoring of open sources of information, will be more fully reflected in the current situation, will help to trace the dynamics of public opinion on any issue.

Data sets, caring public sources are rather huge and also dynamic. Therefore, the composition of the working hypothesis will require considerable time expenses that are required to handle the entire spectrum of the data. When taking into account the economic and political factors we must consider even the smallest changes in the development of the issue in question.

Analysis of open sources will allow estimating the parameters of the "field" in which the company has to work, to identify the strengths and weaknesses of the firm contact of audiences, strategic planning, tactical actions for the development and promotion of products / services.

The use of OSINT can provide answers to many emerging actors in the military and political leadership of the country's issues, and other intelligence agencies to focus on the implementation of more complex and specific tasks without scattering force intelligence.

This type of exploration is typical for the period of the multinational peacekeeping missions because it removes existing barriers to the exchange of intelligence between campaigners from different states. Its role is further increased during special operations, especially when a country wants to hide their involvement in it.

1. Definitions of Open Source Intelligence

The term *Open Source Intelligence* (*OSINT*) is a term that comes from the internal diction of U.S. intelligence. It is since 2002 defined by both the Director of National Intelligence, and the Department of Defense (DoD) as "produced from publicly available

information is collected, exploited, and disseminated in a timely manner to the appropriate audience for the purpose of addressing a specific intelligence requirement"[2].

Open Source Intelligence is represented by all unclassified information, deliberately discovered, and disseminated to a selected audience that addresses a specific question, providing the foundation for other intelligence disciplines. OSINT products can reduce the demands on classified intelligence collection resources by limiting requests for information only to those questions that cannot be answered by open sources.

Open information sources are not the exclusive domain of intelligence staffs. Intelligence should never seek to limit access to open sources. Rather, intelligence should facilitate the use of open sources by all staff elements that require access to relevant, reliable information. Intelligence staffs should concentrate on the application of proven intelligence processes to the exploitation of open sources to improve its all-source intelligence products. Familiarity with available open sources will place intelligence staffs in the position of guiding and advising other staff elements in their own exploitation of open sources.

2. Intelligence and the social networks

One of the new factors that U.S. intelligence is using for analysis work, threat detection and alerts on special crises and risks, is the expansion of social networks, such as Twitter, Facebook, Pinterest and others, who have become a major source of information and; therefore, to develop useful intelligence.

Now, it is taking a step in the exploration of social networks as a source of information to implement projects, and software solutions that enable tracking and early detection of threats. This type of technological applications, some of which are in development and testing phase, either driven by the US Center for Strategic Information and Operations (SIOC),) or Public Resource Center of the CIA (Open Source Center), and also through companies have enormous interest to locate the potentially important information in minutes and issue alerts to detect risk classified keywords, certain facts or events, profiles, people and institutions with potential danger and data requiring a deeper verification.

Information as reported on the networks will not tell anyone who is not a specialist if it involves potentially a threat, that's where intelligence analysts you come into play for you to screen, select and develop useful intelligence in the decision making.

Open Source information (OSINF) is information trawled from the Internet, periodicals, newspapers and radio/TV broadcasts. It is not necessarily free information and includes commercial subscription services like BBC Monitoring or Factiva, and commercial satellite imagery. The main source of information, however, is the Internet. In just 12 years the Internet has grown to become a major source of human knowledge[3]

Intelligence agents can use social networks to carry out transactions of any kinds, in this case the environment is giving them a wide array of experiences and data which is open, very dynamic, stuck to the reality of each country, without having to invest huge sums of money to gather intelligence and conduct security operations and other.

The Convention when examining open-sources considers and reviews the following checklist for each and every open source[4]: Authority – does the source command respect from its peers or customers?; Accuracy – is the source corroborated and benchmarked against other validated all-source material?; Objectivity – does the source advocate or balance views? To

[2] As defined in Sec. 931 of Public Law 109-163, entitled, "National Defense Authorization Act for Fiscal Year 2006".

[3] *See* Clive BEST, "Challenges in Open Source Intelligence", (September 2011): 58-62, accessed August 24, 2014, http://dx.doi.org/10.1109/EISIC.2011.41.

[4] Stevyn GIBSON, *op. cit.* p. 19.

whom does it link? Who or what does it represent? Currency – is it date/time/place/author-tagged for currency?; Coverage – is it relevant (i.e., adds to understanding) or is it just interesting or circular reporting?

Ten years ago, it was unthinkable that U.S. intelligence would be operating with high levels of success with social networks existing back then. Today, it is a reality that social networks allow us to detect threats, neutralize risks, and coordinate attacks from a profile missions, multiple or none, analyzing information and data to understand and anticipate events. Or simply to locate events that are happening and that can affect us. The intelligence that is made with the information obtained from this open source is one of the new resources that allow new technologies and their potential use is only beginning and is unlimited.

3. Private intelligence and open source analysis

It is not surprising that every time you have debate about the need for our politicians to have an intelligence service, arises in society immediate fear that these organizations become instruments of repression or political espionage agencies. Intelligence must be understood within the parameters of doctrine exposed by Sherman Kent, noting that it is knowledge that our men, civilian and military elevated positions, must have to safeguard the national welfare.

The profile of the analyst is someone with intellectual curiosity who likes to discover non-obvious keys behind all information. He/she is someone passionate about an issue not easily understood by us and who comes from various contexts and backgrounds. If you'd like to compare it with music is like having a tree of styles and influences, choosing a director in the movies industry or choosing Linux over windows in the computer industry.

Maybe your issues are not major and they may not be interesting to almost anyone else or raise your social life perspectives. Never mind that. A vocational analyst is a person who knows a lot more on an issue than people just investigating them. A pluri-specialist is someone who enjoys learning and discovering the whys of things and daily news that no one seems to question. He/she is someone whose dream is to get a job where you get paid to read and learn continuously.

Resources of private-information-analytical agency Stratford's, is providing regular updates on areas of deployment of aircraft carriers and expeditionary strike groups of the U.S. Navy, and many more.

Attention should be paid on how to fill these information resources. For example, to collect data from the sites of the World Wide Web, its systematization, transfer and archiving of information in the World Library (World Basic Information Library - WBIL), the operation of which is the responsibility of the management study of the armed forces of foreign states (FMSO) command training and research on Construction Training and Doctrine Command - TRAD-OC), involved personnel of the Army Reserve, and other branches of the armed forces.

Reservists signed individual contracts for a certain number of hours of work per month; everyone gets a free hardware and software that are held for six-hour special online-courses. Thus issued computers may be mounted in any convenient for business and place specified in the contract, including home. It is also clear that this hardware, in effect, is a personal computer for official use that also provides access to the Internet.

As for the organization of consumer access to such information and databases, it has long formed and successfully operated within the United States information society. This allows access quite simply and securely, eliminating the possibility of accidental or unwanted intrusion into information resources that are limited for distribution. To do this, almost all networks require filling out a form indicating the electronic personal data. Sometimes vetting

is required but in most cases only personal information such as the social security number is required.

According to U.S. experts, the development of computer technology, the availability of the Internet and, as a consequence, increase the flow of public information and media allowed to bring the intelligence using open sources of information out of the shadows and make it even more necessary and urgent. The U.S. uses today an open combination of modern technology and intelligence officers have the ability to access vast amounts of data needed to assess the situation, monitor the situation and needs of governments in the data needed to make informed and correct decisions.

Capabilities[5]:

- Potential customer base consists of both Government and Commercial sectors;
- The area of focus is as an information "product" provider driven;
- Products may take the form of reports, alerts, linkages, photos or other images.
- Product value is determined by size of report and time sensitivity of the needed report;
- Government products are delivered as unclassified, but may become classified upon receipt;
- Commercial products are all treated as "company sensitive" regardless of external sensitivities;
- Any need for classified products would be satisfied off site at the customer's appropriate facility utilizing analysts with applicable clearances.

Conclusions

The defence of freedom and democracy needs Intelligence services able to fulfil a preventive mission effectively and efficiently. At present, Intelligence services collect, analyze and evaluate varied information. The reason is obvious: the last two decades have imposed the notion of multidimensional and comprehensive security in a multipolar international order that is identified with the neutralization of military threats from potential enemy states. Not only, are there new and threatening enemies as terrorism, international criminal organizations networks and the proliferation of weapons of mass destruction, but also analysts should pay increasing attention to phenomena linked to the political, social, economic, cultural and environmental threats as, *inter alia*, the expansion of anti-democratic ideologies and fanaticism, the threats of coups, destabilization subversive, genocide, the threats to cultural and community identities, uncontrolled migration and massive conflicts over access to natural and financial resources, the economic espionage, scientific and technological or environmental aggressions.

Today the United States has a strategic intelligence structure that would extract the observation of social phenomena and the scientific analysis to prevent this not be surprised by unexpected situations. The emerging information services have, for the most part, just prepared tactical intelligence, which in many cases, it is not necessary for the driver political strategy to guide the faith of the state.

The realization of the importance of the use of open sources of information and its specific method of administration has not generated; however, the existence of comparable studies in number of and allocation of resources to research aimed at developing technological

[5] "OSINT - Open Source Intelligence," The OSINT Group, August 25, 2014, accessed August 25 2014, http://www.theosintgroup.com/open_source_intelligence.html.

means for obtaining information. Hence the effective management of open source to generate strategic intelligence, or current has become in recent years growing concern intelligence[6].

BIBLIOGRAPHY:

1. BAZZELL, Michael *Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information*. 2 ed. N.p.: CreateSpace Independent Publishing Platform, 2014.
2. BEST, Richard A., and Alfred CUMMING. *Open Source Intelligence (osint): Issues for Congress*. N.p.: Congressional Research Service, 2007.
3. GIBSON, Stevyn. "Open source intelligence." *The RUSI Journal* 149, no. 1 (February 2004): 16-22. Accessed August 24, 2014. http://dx.doi.org/10.1080/03071840408522977.
4. KENT, Sherman. *Strategic Intelligence for American World Policy*. New edition ed. N.p.: Princeton University Press, 1966.
5. MERCADO, Stephen "Sailing the Sea of OSINT in the Information Age." *Studies in Intelligence*48, no. 3 (2007).
6. ***, *Words of Estimative Probability*. N.p.: Central Intelligence Agency, 2012.
7. "DNI - Director of National Intelligence." September 1, 2014. Accessed September 1, 2014.http://www.dni.gov.
8. "OSINT - Open Source Intelligence." The OSINT Group. August 25, 2014. Accessed August 25, 2014. http://www.theosintgroup.com/open_source_intelligence.html.

[6] Stephen MERCADO, "Sailing the Sea of OSINT in the Information Age", *Studies in Intelligence* 48, no. 3 (2007).

EVALUATION OF COMBAT FORCES FOR PARTICIPATION IN COALITION OPERATIONS

Cristinel Dumitru COLIBABA
PhD candidate, Commander, 280th Mechanized Infantry Battalion.
E-mail address: cristicolibaba@yahoo.com

Abstract: *Evaluation as process measures in detail performances and capabilities of a Land Forces unit nominated for participation in a mission abroad usually within alliances or coalition with the single goal to provide information pertinent to unit readiness, a statement of the unit' current ability to perform its mission.*

Either formal or informal, evaluation is a continuous process that allows the commander to assess the unit's proficiency in the essential tasks and to validate the effectiveness of the unit's training plan. The commander reviews the training deficiencies of subordinate units and individuals, and adjusts the training priorities in the unit's training plans accordingly in order to meet the expected state of readiness.

Keywords: *training evaluation, assessment, after action review, training.*

Introduction

The Land Forces must always be ready to conduct successful combat operations. The main purpose of training is to prepare soldiers and units to fight and win in combat.

Because Land Forces units cannot achieve and sustain peak proficiency in all possible mission tasks, commanders are required to identify those tasks essential to their unit' wartime mission. The resulting list of mission's essential tasks forms the basis of the commander's unit training and evaluation program.

Training evaluation is an integral and essential part of the training cycle, since it tells commanders how proficient their units are in mission-essential tasks. In this way, the evaluations also provide the basis for commanders to plan future training.

Evaluations of training conducted by Land Forces units provide information to commanders on their units' capacity to meet the performance standards settled for successful combat operations. This is why training evaluation is an essential part of training.

1. Importance of training

Successful combat units train as they fight and fight as they train. This is the foundation of unit training.

Training evaluation is integral to training management and is conducted by leaders at every level.

Regarding this, there are questions that commanders hope to find god answers for: Has the training met the predetermined expectations? Is the unit better able to accomplish its mission? How can we improve the training? Is the amount of resources satisfactory to accomplish the mission?

2. Evaluation – commander's tool to assess unit readiness

The commander needs a tool for that. The tool stays in a good evaluation process and a good assessment of his unit's training readiness based on a real platform which replicates as best as possible the "real world" meaning a very good image closest to that in operational theater.

Because home-station training for Land Forces units generally lacks realism and evaluators use ambiguous criteria and may not be objective, evaluation results do not provide reliable information about units' proficiency to perform wartime missions. Moreover, training readiness assessments of Land Forces units may be overstated, and the information provided to higher commands is of limited value because the assessments are based on training conducted primarily at home stations and may not adequately consider all the aspects with influence on proficiency such as of the loss of key personnel, employment of a credible opposing force, use of minimal or no smoke, generally did not include CBRN training, and did not incorporate elements of combat service support.

A Commander's initial and ongoing training evaluation will be framed by his assessment of unit proficiency in those collective tasks derived from an analysis of the unit METL and defined by the tasks, conditions, and standards articulated in the unit's standards document(s). Each evaluation should be tailored to assess progress toward attaining the commander's training goals and achieving combat readiness prior to deployment. Commanders and subordinate leaders are responsible for evaluating their units and subunits to identify strengths and weaknesses, and to make corrections to the unit training plans and priorities to focus training and training resources effectively and efficiently.

Evaluation is a continuous process that occurs at all echelons.

Both informal and formal evaluations of training are necessary to ensure that Land Forces units are prepared for combat.

Informal evaluations should take place during all scheduled training, regardless of the size and scope of the exercise. Individuals and units should be evaluated daily as they conduct routine training or perform day-to-day missions. Leaders at all levels evaluate training performance and provide feedback to the chain of command, trainers, and those being trained. Informal evaluation of training also provides an opportunity to ensure proper techniques, tactics, and procedures have been instructed and learned.

Formal evaluations are often scenario-based, focus on the unit's mission-essential tasks, and use collective training standards as the criteria to assess unit proficiency. Formal evaluations determine an individual's or unit's proficiency in the essential tasks that must be successfully performed in combat.

Formal evaluations should be planned and scheduled as part of the construction of the unit's training plan. After Action Reviews (AAR) of formal evaluations, are used to determine better means for accomplishing objectives, allocate future resources, improve individual and unit performance, develop qualified trainers, and make appropriate adjustments to the unit training plan. Organizations conduct AARs to identify successes and challenges and apply observations, insights, and lessons to future training and operations. If necessary, organizations conduct AARs after intermediate actions are completed, not just at the end of the event. Training helps correct deficiencies identified during operations. AARs provide an excellent opportunity for units to reinforce the development of critical thinking in leaders. As an integral part of unit training, AARs help establish a learning environment where successes and honest mistakes are freely discussed among leaders, participants and observers. AARs provide a medium for units and individuals to understand what went right, what went wrong, and what could be done better in future training and operations. Sharing observations and lessons learned during the AAR and referring back to the training objectives established

during planning helps units determine task proficiency and mission success. AAR discussions must facilitate future improvements in unit performance as they perform the same or similar tasks again during future training or operations.

3. Realistic assessment based on training infrastructure and evaluation management

Speaking about platform, The Land Forces Combat Training Center (LFCTC) provide the most realistic environment available for unit training during peacetime and the most comprehensive, objective evaluation of unit proficiency.

The LFCTC require units to conduct operations over 5 to 7 days in an environment very similar to that of actual warfare-an opportunity not generally provided at home stations. Force-on-force exercises at the LFCTC the Multiple Integrated Laser use Engagement System (MILES) to increase realism and objectivity. This system, which is carried by troops and mounted on equipment, instantly informs soldiers and units of a "kill" or "near-kill." MILES enables commanders to see immediately the results of their orders and tactics.

Units can also take advantage of training simulation to improve and evaluate proficiency. Simulations offer effective training alternatives when maneuver and gunnery opportunities are limited. They provide information that can be used to evaluate individual and unit proficiency and to identify training needs.

Simulations, in general, do not provide a fully adequate substitute for traditional field training, but they do provide a realistic supplement. In some cases, however, a simulation may be preferred over traditional field training.

Over the past decade, overseas deployments have reduced training timeframes and resulted in senior leaders assuming training management responsibilities from junior leaders. Specifically, leaders at higher headquarters have taken responsibility for much of the training management function— planning, preparing, and assessing training—while junior leaders have focused primarily on training execution. Changing conditions, such as competition for resources in a constrained fiscal environment and a return to training for a fuller range of missions, make it imperative that all leaders possess a strong foundation in training management.

The main rehearsal exercise (MRE) is intended to challenge units and their leaders in an environment that involves scenarios that replicate current operational conditions in the theater to which they will be deploying.

Proficiency in mission-essential tasks demonstrated under more realistic conditions at LFCTC provides a more valid indication of unit readiness. It was observed that external evaluations are not as thorough or objective as called for by training guidance and evaluation comments are often influenced by the evaluators' desire not to damage a commander' image by highlighting significant weaknesses that are often discussed informally but not included as part of a formal evaluation report.

In some cases, LFCTC results are used as the external evaluation of units results offer a more valid indication of proficiency because LFCTC provide more realistic training and more thorough and complete evaluations.

The LFCTC provide highly realistic wartime environments that cannot be created at most home stations. As a result, unit proficiency is evaluated under conditions similar to those under which missions would actually be accomplished.

Units train against dedicated and well-trained opposing forces at the LFCTC, thus ensuring that they are evaluated while confronting a formidable force.

Units must demonstrate their sustainment abilities at LFCTC. Under realistic combat conditions, units have to provide full logistical support performing maintenance in the field,

evacuating casualties, replacing lost personnel, and replenishing all items consumed during operations.

Units are evaluated by a large cadre of independent, well-trained observers/controllers. LFCTC evaluations are also enhanced by audio, video, and computer systems in place to record objective training data.

Training realism at the LFCTC is believed to be too challenging due to, opposing forces encountered at the LFCTC are more formidable than any hostile force the units are likely to face in actual combat, and the stress faced by soldiers and leaders at the LFCTC is more demanding than that in real warfare.

Commanders assess each training event through a lens focused on execution within the commander's intent, achievement of the training objectives, and progress towards full spectrum operations METL proficiency. The training meeting is the best forum to aggregate evaluations of tasks by subordinates and the commander into the full spectrum operations METL assessment. Commanders assess mission-essential tasks as T—trained, P—needs practice or U—untrained.

Based on these assessments, commanders adjust their future training plans as needed. Training assessments also address such areas as training support, force integration, logistics, and personnel availability. These assessments form the basis for determining the organization's training ratings for readiness reporting.

Criteria used to determine proficiency in mission-essential tasks are too general to ensure consistent assessments among units. Doctrine prescribes a standard set of criteria- "trained", "needs practice," and "untrained" -for commanders to use in assessing critical task proficiency of both active and reserve component units. Army training regulations define these criteria as follows:

"Trained. The unit can successfully perform the task to standard. Only sustainment training is needed. The leader judges task performance to be free of significant shortcomings. Practice on "T" tasks are designed to keep soldiers from losing proficiency."

"Needs Practice. The unit can perform the task with some shortcomings. The shortcomings are not severe enough to require complete retraining. Only refresher training is required."

"Untrained. The unit cannot perform the task to standard. The leader prepares a comprehensive strategy to train all supporting tasks not executed to standard."

These criteria require commanders to exercise considerable judgment. Depending upon a commander' personal interpretation of "significant," "some," and "severe," critical tasks could be assessed as "trained," "needs practice," or "untrained" and result in a training proficiency assessment different than that of a unit of similar proficiency.

Basing training readiness assessments primarily comes upon a limited number of mission-essential tasks conducted under artificial training conditions at home stations may overstate units' training readiness. Also, failure to take into account substantial changes in key personnel or reductions in training opportunities following a LFCTC visit further decreases the validity of unit readiness reports.

Conclusions

Because of the wide latitude commanders can exercise in assessing training proficiency, the Army has no assurance that these assessments are consistent from unit to unit. Moreover, the latitude of interpretation does not provide higher levels of command a full understanding of unit proficiency for tasks assessed as "needs practice." Depending upon the commander' interpretation, the meaning of an assessment of "needs practice" for a mission-essential task could range from only a limited number of subtasks to the majority of subtasks

not performed up to standards.

Deploying Land Forces units conduct extensive pre-deployment training—both individual and collective, to include a large-scale main rehearsal exercise (MRE) at Land Forces Combat Training Center. However, the current focus on counterinsurgency operation training have been preventing units from completing all desired training prior to the main rehearsal exercise (MRE). For example, units were not able to complete all of the desired individual and collective training prior to arriving at the combat training center since resources—such as theater-specific equipment like mine resistant ambush protected vehicles—were more readily available there.

According to trainers at the combat training center, while units arrive with varying levels of proficiency, all forces leave with at least the platoon level proficiency required to execute the counterinsurgency missions required for ongoing operations in Iraq and Afghanistan.

Basing training readiness assessments on LFCTC exercise evaluations that provide more realistic and challenging training would be a better indicator and provide more complete and reliable information to higher levels of command. To achieve this result and facilitate analysis, however, some modification to the structure of LFCTC take-home packages will be needed and the commander bases a subjective assessment on observed task proficiency and whether training met objectives and supported full spectrum operations METL proficiency.

BIBLIOGRPHY:

1. FM 7-0 Training units and developing leaders for full spectrum operations, Headquarters Department of the Army, February 2011.
2. GAO, Report to the Chairman, Subcommittee on Readiness, Committee on Armed Services, House of Representatives, Army Training, Evaluations of units' proficiency are not always reliable, February 1991.
3. GAO, Report to the Chairman, Subcommittee on Readiness, Committee on Armed Services, House of Representatives, Army and Marine Corps Training, Metrics needed to assess initiatives on training management skills, July 2001.
4. MCO 1553.3A, Unit training management, Washington, DC, 22 Jan 04
5. SMG/Ctr.1- Instrucţiuni privind evaluarea capacităţii unităţilor/detaşamentelor din Forţele Terestre participante la misiuni în afara teritoriului statului român, Bucharest, 2008.

CULTURE, INTERCULTURALITY AND MULTICULTURALITY WITHIN THE ISAF HQs

Rita PALAGHIA
Civilian Assitant at NATO HQ ISAF Kabul, Afghanistan.

Abstract: *The raise of the importance of the cultural identity and of the inherent frictions generated by this determine the need for all the military and civilian leaders of the understanding of the cultural and societal norms of the population where it functions and operates.*

ISAF represented over the years not only a test for NATO, but it showed the relevance of the organization within the contemporary security environment.. Operating over the last Decade, ISAF increased its presence and experienced a serial of enhancements related to the development of NATO Doctrine for stability operations and counterinsurgency. This analysis is done base don the need to understand the way different cultures inside ISAF are inter-related and they are developing efficient functional mechanisms in a military multinational Environment, within the Afghan Theatre of Operations. This interest was generated also by the fact that Romania is taking part to the Mission with military forces, not only in Regional Initiatives, but also in different Theatre of Operations, inside some Observer Missions.

Keywords: *culture, interculturalism, multiculturalism, NATO, International Assistance Security Force.*

1. Theoretical approach

UNESCO is considering culture as „*a series of distinct features of a social group or a society, regarding the spiritual, intelectual or emotional terms”*. A simple definition of culture might be also as „*unwritten rules of a social game*”.

Geert Hofstede is defining culture as "*mind collective programming that is making distinction in between the members of a group or category of persons from another group or category*". "Category" is referring to nations, regions inside or outside of a nation, ethnic group, occupation, organization or gender[1].

A sub-culture is proposing either a group of simbols, norms, values or non-identical ways of life with those dominating culture in a society, nor in antagonism with these, but additional to them. Being conscientious about the ambiguity of the cultural term (that has the co-notation of something that is subordinated to a dominant culture, that has an underground character), Ulf Hannerz is proposing a rethinking of the sub-culture as an integral part of a larger system, that is differentiating it from the interior, which is formed as a relationship network and social situations, where in between the participants it is articulating a symmetry of perspectives. While it is recognized the heterogeneity character of the sub-cultures, we need to be conscientious of that their delineation is relative and the limits in between them are evolving permanently. In his opinion, the classification and the self-classification of people in sub-cultures is serving to express the social distinction and to the consolidation of the cohesion of a group.

[1] Geert Hofstede, Gert Jan Hofsteden Michael Minkov, „Culturi şi organizaţii. Softul Mintal, Cooperarea interculturală şi importanţa ei pentru supravieţuire”, Editura Umanitas, Bucuresti, 2012.

Multinational military operations comprise participants with a different style of thinking that can perceive differently a particular situation. A multinational Army is not normally homogenous from the cultural point of view. Moving from macro to micro level, we are discovering a variety of sub-cultures, which are differentiating themselves from the structural and geographical point of view. Structural sub-cultures seem to be different: horizontally, in between services and vertically in between different categories of personnel, as are for example, the vertical classical structure in between officers and NCOs.

The concept that is illustrating in an adequate manner, what is happening now inside the Societies is called „Interculturality", where the term „inter" is suggesting interaction, the change and the ultra dynamic character of the societies in which we are living, a concept that is making us thinking to reciprocal exchange and dialog. Interculturalism is the exchange philosophy in between cultural groups. Some states have inter-cultural policies that are encouraging socializing of the citizens having diverse origins, being often used as a fighting instrument against racism, preconceived perceptions or misunderstanding of those belonging to other cultures.

Interculturalism imposes an inherent openness of cultures. Once a group of persons is exposed to the elements of a different culture, then a dialogue will be set up to identify common elements. In time, through this fusion of the common elements, a new type of culture is developing. The differences that will remain will form the subcultures.

Multiculturalitaty is an intrinsic term for the historical evolution of the Humanity. It is normal that this term is to be associated with the characteristics and the specificity of the groups, reflecting the variety of the cultures that are manifesting themselves in the same space and time, without being absorbed one into another. Those different types of cultures are living their own moment, avoiding any influence. (Rey, 1999).

Multiculturalism is a term often used within the context of public policies aiming to manage the cultural diversity in multi-ethnic organizations and societies, having as central element the mutual respect and tolerance, inside the societal and organizational framework. (La Belle, Ward, 1994, p.15). The term used for the first time in 1957, aiming to describe the Swiss Society, being used also in Canada, starting with the End the 1960s, later on being spread among the native English speaking countries (La Belle, Ward, 1994). Staring in the 1970s, multiculturalism began to be incorporated in social politics of different countries, for reasons that were different from a country to the other.

The term „Multi" is confusing the term „race" and „culture". The term "race" does not mean anything, at a detailed analysis. It is agreed that, in „DNA" terms, the race" does not have a significant role, as the other attempt to categorize the human differences. „Multiculturalism" has found a proper way to become popular, because the „race" is not defining a real difference in between people, but the way in which persons are evolving, with their system of values and believes that is making the difference.

Multiculturalism in an ideology that is affirming that the Society has to be formed, or at least to allow to include distinct cultural groups having the same equal distinctive status with the other members of the Society. If they have to have or not the same distinctive political status is still a subject for discussion among those that are studying the political science. Some nations had adopted favorable social policies to the concept, but the norms are varying according to the cultural diversity with its variable degree of tolerance and acceptance. The term "multiculturalism" is also used to describe the demographic conditions of the appearance of ethnic and cultural diversity, no matter if it is supported or not by social policies.

There are a lot of benefits provided by multiculturalism. From the mixture of the cultures new ideas will appear, that will be useful for everybody. If we will not have that, we would not have the experience of the variety that generates the differences. With those ideas

and believes, we are developing respect for the way we think and interact, and we will learn from them. If we are suppose not to have multiculturalism, we will be all the same, will have the same system of believes and behavior. This, probably will function very well in a reduced in size society, but the element called creativity, probably would be very dominant. It is possible that this type of society to be blocked in time, having an extremely reduced evolution.

2. Multiculturalim within NATO

The inherent multiculturalism within NATO is representing an important advantage in portraying a positive image of the Alliance. Understanding the way in which people are procuring information and the adaptation of the message to the public level target audience are the basic elements of an efficient communication. As an Ideology of Diversity, multiculturalism has the task to offer a form work of reaffirming or portraying the group identity. Multiculturalism it seems to respond to the need of a World in changing in which, is in a form of answers to the challenges brought by the National State, both in trans-national and global spheres. Thus, the Globalization Process is forcing us to adapt the majority/minority ratio, in specific cultural space at the global level, asking us for understanding, acceptance and affirming the diversity.

Understanding the cultural aspects in a specific multinational environment is starting with local history, religion, culture, customs and laws. A profound understanding of the operational environment needs the understanding of the roles of the whole actors participating in the Area of Operations, that are combining in order to create a living organism of cultural knowledge. These have to be updated on a permanent basis and enriched in time, using direct and indirect sources of information. The direct knowledge is obtained through direct interaction with people. The indirect knowledge is obtained through research and study, and then it is checked using interaction and monitoring the local population. ISAF has found out too late that cultural knowledge is absolutely critical.

Despite this, the „internationalization of the military life" in the last twenty-five years led to new organizational challenges. The collaboration in between different armies and branches, information and communication needs technological interoperability but also the adaptation to the multinational environment, with different languages, different styles of leadership, rotational systems, training, military traditions, hierarchy systems etc. Thus, the interaction inside a socio-technical system is very difficult, because the structure, people, persons and cultures are aligned in order to attain the objective and they are essential in accomplishing the mission in an efficient manner. Multinatinationality of those Coalition operations is blocking sometimes organizational efficiency. In order to attain and to maintain the organizational efficiency at a higher level of adaptation, we need flexible and mobile forces. NATO is accomplishing this challenge trough a transformation process underlining „the reduction in size and availability"," increased mobility and flexibility" and of „ multinationality".

The cultural and religious problems are influencing peacekeeping operations in two ways. Firstly, the soldiers of the multinational forces, that is coming from a variety of cultural environments and has to manage those cultural differences amongst them in order to work efficiently. Secondly, the soldiers have to adapt their own style of working to the local operational conditions in order to keep the good relationship with the local population. The initial assumption made is that a successful cooperation in between NATO soldiers will be easier because they are sharing the same fundamental values and they could have even a certain previous experience in working together. Despite those, the research is suggesting that cultural and religious differences might lead to tensed relations and to the decrease of the

efficiency. Indeed, the research done now that are examining cooperation in between the Dutch and German troops in Afghanistan by Sjo Soeters and Ren Moelker from Dutch Royal Military Academy from Breda, indicated that despite the perceived cultural differences, the working relations proved to be a problem from time to time. This was in contrast with the good Dutch-German cooperation in Muenster, Germany.

Understanding national differences can improve the efficiency in multinational coalition operations. This aspect can be tackle in two distinct ways. Firstly, you need to achieve the increase of the efficiency of the military personnel that will take part into multinational operations. This is a critical issue because the operational efficiency is depending of the development of a common ground in between the members of a team. Secondly, it has to inform correctly the system to support the decision making in a cultural environment that has differences in terms of motivation, judgement and power structure.

Despite the fact that the Allied soldiers are bringing different national military traditions inside the Coalition, the military profession has a matrix with common dimensions.

The anthropologic research has underlined that the language, social norms and customs are associated with the national cultures. Language is essential in communication. The International Aviation has recognized the importance of a common language adopting a standardized language system in using the messages. This is vulnerable when the events that are complex, unexpected and has not be seen before, have to be described. The common language remains a problem in all domains, including the participants to multinational missions. Even the native English speakers are reporting some confusion when they are sharing complex information with the other non-native English Language speakers.

The behavior, rules and customs are also important within multinational collaboration. Cultural sensibility to the social norms and customs is still important for the Allied troops because they can generate negative feelings that can put in danger the direct contact of the soldiers with the local population, being in the position to neglect or not to respect the social norms and customs. Because the behavior is barriers, they got a considerable attention within NATO forces. Understanding behavior it is not sufficient in order to ensure the efficiency in multinational operations.

The cultural values are transmitted from the social perspective from generation to generation and they are different from one nation to the other. Kluckhohn and Strodtbeck (1961) had developed a framework to understand the variation of the valoric orientation inside a specific culture. One of those dimensions, the orientation activity, is making the difference in between the self restraint o none side and the confrontation status, on the other side.

Cultural differences related to knowledge (i.e. Cialdini, Wosińska, Barrett, Butner and Gornik - Durose, Faure, 1999; Gelfand & Christakopoulou, 1999; Harris & Bond, 1999) are critical in multinational operations[2]. Those can act against the common perception, to the sustained communication and to the coordinated actions (Radford, Mann, Ohta, Nakane, 1993). The cognitive activity is offering the foundation for the individual perception, evaluation, judgement and action. In coalitions, the participants have to predict the decisions and actions, to maintain communication and to coordinate their actions.

The multinational military operations include participants that are having different styles of thinking and they can see differently a situation. In contrast with the behavior and social differences, the cognitive ones can not be observed directly. Planning and coordination will be frustrating and risky when we are in the position not to anticipate the reactions, or, even we can do that, the confusion is probably to appear.

[2] E. Hutchins. Cognition in the Wild. MIT Press, Cambridge, MA, 1995.

The socio-cultural factors can influence the decision of a Nation in using the mandatory recruitment or the voluntary option in order to generate the human resources, the way in which the public opinion is managing the issue of casualties, and also the measure in which the public opinion is supporting the accomplishment of the military mission. The word recruitment itself, involves the lack of a choice. From the historical perspective, during the war, some countries relied on recruitment in order to satisfy the human military needs, while others used a variation of this process. USA and Canada, even they are aligned culturally in a way, used different forms of recruitment, for different objectives. Other nations like Australia, Israel, France, Spain, Italy and Germany, had adopted the mandatory recruitment, guided by their culture, history, economy and their own political systems. Even the research is showing that socio-economic factors from those two approaches of the military mobilization process could bring tensions and may threat the cohesion within a multinational context, a good leader can be in the position to resolve most of those problems, especially using the concept of belonging to the military ethos, a concept that is shared by many cultures and nations (Elron et al., 1999). The acceptable tolerance of a number of casualties is flexible and is varying according to the duration of the military operation and according to its associated costs[3]. The war in Irak is an example especially fro the US point of view, a case in which the initial tolerance related to the number of seemed bigger, but dropped in time. In a similar way, the public response in the case of Canada during the war in Afghanistan has fluctuated in time, duet o the change in the tolerance related to the casualties.

The Australian approach related to the participation with forces to the mission is transmitting a certain level of tolerance, regarding the losses, which could be in contradiction with other national contingents that are suffering higher casualty numbers.

Related to the wars in Afghanistan and Irak[4], it seems that there is a shared opinion in the International Arena, but is not unanonimous, making those wars unpopular. There is a cross-cultural link, that is indicating that the public opinion of the countries that are having National Contingents in the Theatre of Operations, are determining in a greater measure, the level of implication of those nations in terms of the multinational mission, the size of the contingent and the duration of their involvement.

Public opinion is a social key indicator of Foreign Policy that is influencing the way in which the leaders are responding to the reaction of the population. In the case that National Contingents do not have the support of their own population, then their role inside the multinational Coalition Forces can become a problem, not only for their Government, but for the conduct, the efficiency and the results achieved by accomplishing the mission.

Conclusions

Instead of conclusions and proposals, I would like to mention that culture should be seen as a moderator for the psychological effects, or very often as something that is fundamentally changing the Human Nature. Cultural differences are natural and they have to exist. Most of the human behavior is universal, not cultural.

If we do not look for cultural differences, we will build our own obstacles, but if we will be looking for similar cultures, then we will build links and a stable favorable foundation for the future military cooperation. Cultural differences are enriching the experiences gained in a specific country, but they are representing rarely a factor that is fundamentally changing the human psychology or the basic principles of War.

[3] King, Anthony (2006).The Word of Command: Communication and Cohesion in the MilitaryArmed Forces & Society,Vol.32,No.3,(April 2006),493–512.
[4] Forster, Anthony (2006). Armed Forces and Society in Europe. Palgrave Macmillan, Hampshire.

The measure in which a cultural phenomenon needs an explanation is depending of the received operational task. On one hand, if it is clear that this phenomenon will influence the operations, then, using all the means possible, it should be included in the functional planning process. On the other hand, in case that the culture does not influence the operational task, then it should be left as a task for the anthropologists.

The ignorance can have deadly consequences. NATO led Coalition Forces are pretending that in the last years the Afghans had killed thousand of Coalition soldiers. Their first reaction was to blame the Talibans, but in reality the majority of those killings are duet o cultural differences and misunderstandings.

There is no doubt that cultural differences are representing an important barrier inside the command and control process of the Coalition and this is because of the complexity of the National Cultures. Cultural understanding and knowledge, both inside the Coalition and within the interaction in between NGQs and local population, are offering a possible anticipation of the actions, the elaboration of correct and valuable judgments and also the efficient negotiation of the differences. A cultural objective that is clearly understood and achieved will consolidate the path in this context.

The results of some studies are revealing that verbal communication, reciprocal understanding, friendship, openness and societal competencies are basic conditions for a successful cooperation in between military personnel. Learning how to interact, both with the local population and inside the Coalition, is representing a major challenge, both for leaders, civilians and for military personnel.

We can not say that within ISAF HQs interculturality is existing. The frequent rotation of the soldiers coming from different cultures does not creating the proper environment for a cultural exchange and of a joint, unique culture.

"The brochure for cultural understanding of „Coalition Forces" having 28 pages and that it was distributed to nearly 5,000 Afghan soldiers so far, is bringing a clear picture over the huge cultural gap that is still existing after so many years of common fighting against Talibans. In an extremely religious country, that is having a culture of honor and pride, the guide is presenting the Allied soldiers behavior that can be considered as „sacred" subjects. „*Therefore, in this context, even the little cultural differences can generate disputes and misunderstandings*".

BIBLIOGRAPHY:

1. BARAM, Amatzia, "Victory in Iraq, One Tribe at a Time," New York Times, Oct. 28, 2003. Available at: http://www.nytimes.com/2003/10/28/opinion/28BARA.html.
2. BHATIA, Michael, 'Shooting Afghanistan–Beyond the Conflict,' The Globalist, accessed at www.theglobalist.com/StoryId.aspx?StoryId¼6417. Michael Bhatia was killed în Afghanistan on 7 May 2008; he was an extraordinary humanitarian and humanist, a profound thinker about humanitarian intervention, and a cherished friend and colleague.
3. BURNS, John F., "The Reach of War: The Occupation," New York Times, October 17, 2004. Gen. Kennett appears to be paraphrasing T. E. Lawrence: "Better let them do a poor solution than you presenting the best. For theirs is the land and the future and your time is short."
4. CANNON-BOWERS, Janis A.; SALAS, Eduardo, Individual and team decision making under stress: Theoretical underpinnings. In J. Cannon-Bowers and E. Salas (Eds), Making decisions under stress: Implications for Individual and Team Training, p. 17-38. American Psychological Association, Washington, D.C., 1998.

5. CASTRO, Carl A. (Eds). (2006). Military life: The psychology of serving în peace and combat.Vol.4, Military Culture. Westport, CT: Praeger Security International; Greenwood Publishing Group, Inc. Chapter 2, 13–34.
6. CLAPPER, James R. Jr., "The Worldwide Threat to the United States and its Interests Abroad," Statement to the Senate Committee on Armed Services, January 17, 1995. Available at: http://www.totse.com/en/politics/terrorists_and _freedom_fighters/wrldthrt.html.
7. CLARK, T.; JONES, R. (1999, June). Organizational interoperability maturity model for C2. In CCRP, proceedings of the command and control research and technology symposium, Newport,RI, USA.
8. CLOVER, Charles, "Amid Tribal Feuds, Fear of Ambush and the Traces of the Colonial Past, UK troops face up to Basra's Frustrations," Financial Times (England), September 6.
9. ELRON, Efrat; Shamir, Boas; Ben-Ari, Eyal (1999). Why Don't They Fight Each Other? Cultural Diversity and Operational Unity in Multinational Forces. Armed Forces & Society, Vol. 26, No. 1, (Fall 1999), 73–98.
10. HALTINER, Karl W.; SZVIRCSEV Tresch, Tibor (2006). Phänomen «Militär» – Eigenschaften einer eigenartigen Organisation. In: Annen, Hubert, Zwygart Ulrich (2006). Das Ruder in der Hand. Aspekte der Führung und Ausbildung in Armee, Wirtschaft und Politik. Festschrift für Rudolf Steiger. Huber & Co.Verlag: Frauenfeld, 193–202.
11. HEIBERG, Marianne, 'Peacekeepers and Local Populations: Some Comments on UNIFIL', în Indar Jit Rikhye and Kjell Skjelsbaek (eds) The United Nations and Peacekeeping: Results, Limitations, and Prospects: The Lessons of 40 Years of Experience, London: Macmillan, 1990, pp.147–69. See also Tamara Duffey, 'Cultural Issues în Contemporary Peacekeeping', International Peacekeeping,Vol.7, No.1, 2000, pp.142–68;
12. KATZENSTEIN, Peter J., The Culture of National Security: Norms and Identity in World Politics, New York: Columbia University Press, 1996; Colin S. Gray, Nuclear Strategy and National Style, Lanham, MD: Hamilton, 1986.
13. KLEIN, Paul; HALTÎNER Karl W. (2005). Multinationality as a Challenge for Armed Forces. In: Caforio, Giuseppe; Kümmel, Gerhard (eds.) (2005).
14. KLEIN, Paul et al. (2005). Multinationality as a Challenge for Armed Forces.
15. KLEIN, Paul; KÜMMEL, Gerhard (2000). The Internationalization of Military Life. Necessity, Problems and Prospects of Multinational Armed Forces. În: Kümmel, Gerhard; Prüfert, Andreas D. (eds.) (2000).
16. LEEDS, Christopher A. (2001). Culture, Conflict Resolution, Peacekeeper Training and the D Mediator. International Peacekeeping, Vol. 8, No. 4, (Wînter 001), Taylor & Francis Ltd, London, 92–110.
17. LANE, Sandra D.; RUBINSTEIN Robert A., 'Judging the Other: Responding to Traditional Genital Surgeries', Hastings Center Report, Vol.26, No.3, 1996, pp.31–40.
18. LIPCHITZ, R., On-line coping with uncertainty: Beyond reduce, quantify and plug heuristic. In R. Flin, E. Salas, M. Strub, & L. Martin (eds), Decision Making Under Stress. Ashgate Publishing, Aldershot, England, 1997.
19. LIU, Melina, "The Will of the Tribes," Newsweek, March 17, 2003.
20. PENG, K.; NISBETT, R., R. Culture, dialectics, and reasoning about contradiction. American Psychologist, 54, 741-754.
21. RADFORD, M.; MANN, L., OHTA, Y.; NAKANE, Y., Differences between Australian and Japanese student's în decisional self-esteem, decisional stress and coping styles. Journal of Cross-Cultural Psychology, 24, 284-297, 1991.

22. RUBINSTEIN, Robert A., 'Intervention and Culture: An Anthropological Approach to Peace Operations', Security Dialogue, Vol.36, No.4, 2005, pp.527–44; 'Culture, International Affairs and Peacekeeping: Confusing Process and Pattern', Cultural Dynamics, Vol.2, No.1, 1989, pp.41–61.
23. SAHNOUN, Mohamed, Somalia: The Missed Opportunities, Washington, DC: United States Institute of Peace Press, 1994. These all treat local cultural factors in relation to UN efforts in Somalia. On the importance of local culture to UNTAET, see Tanja Hohe, 'Clash of Paradigms: International Administration and Local Political Legitimacy in East Timor', Contemporary Southeast Asia, Vol.24, No.3, 2002, pp.569–89;
24. SOETERS, Joseph; Winslow, Donna J.; Weibull, Alise (2003). Military Culture. In: Caforio, Giuseppe (ed.) (2003). Handbook of the Sociology of the Military. Kluwer Academic/Plenum Publishers, New York, 237–254.
25. SOETERS et al. (2006). Smooth and Strained International Military Co-operation.
26. TRIANDIS, H.. Culture and Social Behavior. McGraw-Hill, New York, NY, 1994.
27. TVERSKY, A.; KAHNEMAN D.. Judgment under uncertainty: heuristics and biases. Science, 185, 1123-1124, 1974.
28. VAN RUITEN, Schelte (2006).Who is We? Narratives Regarding Trust, Identity and Co-operation within 1 (GE/NL) Corps. In:Vom Hagen, Ulrich;
29. VEDDER, M, Engaging the Female Populace, Proposal for Military Females to Engage Afghan Females. Public Intelligence, available at http://publicîntelligence.net/isaf-afghan-female-engagment-teams-proposal
30. VLAŞIN, Ioan, „Competency, A qualitative participation at anybody's hand", Unirea, 2013.
31. ZSAMBOK, C.; KLEIN G., Naturalistic Decision Making. Lawrence Erlbaum Associates, Inc., Mahwah, NJ, 1997.
32. Department of Defense, Quadrennial Defense Review (QDR), September 30, 2001.
33. Cultural Interoperability: Ten Years of Research into Co-operation in the First German-Netherlands Corps. Sozialwissenschaftliches Institut der Bundeswehr. Forum International. Volume 27. Breda & Strausberg, 131–161.
34. Military Missions and Their Implications Reconsidered: The Aftermath of September 11th. Contributions to Conflict Management, Peace Economics and Development, Volume 2, Elsevier Ltd.: Amsterdam, 403–414.
35. Military Sociology. The Richness of a Discipline. Nomos Verlagsgesellschaft, Baden-Baden, 311–328.
36. United Nations (2007). United Nations Peace Operations. Year în Review 2006. http://www.un.org/Depts/dpko/dpko/pub/year_review06/
37. http://www.army.mil/profesşionalWritîng/volumes/volume3/june_2005/6_05_3_pf.html
38. ISAF Homepage, available at: http://www.isaf.nato.înt/history.html.
39. ISAF Homepage, available at: http://www.isaf.nato.înt/mission.html.
40. http://www.pitt.edu/~kis23/1310-Jan12.pdf accessed 0702006.

PEACEFUL WOMEN AND WORRIOR MEN. A GENDER PERSPECTIVE ON WAR AND SECURITY

Ilona VOICU
Sociologist with Social and Behavioral Studies Centre, Ministry of Defense, Romania.
E-mail address: ilona.voicu@yahoo.com

Abstract: *For a long time, the right to participate in war was a male prerogative, women participation in the military actions being, over time, only exceptional events. Even if this situation seems to be changing nowadays, considering the acceptance of women in the modern armed forces, there are still some controversial aspects regarding the connections between women and security related issues, which this paper is trying to emphasize. In the first part, will be discussed some gender stereotypes on the relationship between women and the military environment, and in the second part will be presented a critical analysis about the approaches of international organizations (UN and NATO) on gender mainstreaming in security policies. Finally, the paper will present the key ideas and a few conclusions.*

Keywords: *gender relations, stereotypes, UNSC 1325 Resolution, women security, gender mainstreaming.*

1. Gender stereotypes and military conflicts

The separation between war and women represents, otherwise, a particular expression of a gender stereotype according to which women are related with nature and peace, because they give life, while the men, according to their aggressive nature, are designated for the military fight. In reality, it is a stereotyping perspective "of peaceful women and belligerent men which affects the ways we view the interests of men and women have with regard to the issues of defense and security"[1], and consequently, according to this type of dissociation, present not only in the common perception, but also in some theoretical approaches regarding International Relations[2], women are not or it is not beneficial for them to be interested in security policies.

The dissociation between women and war could operate in many ways. A first one is represented by the fact that the word *woman* is used as comparative term, as "the other", in the process of building the fighter identity. Often, during the training process, the soldiers who don't correspond to the exigencies are named by their instructors "woman". In consequence, to be a woman has a pejorative connotation, still from the period when the professional identity built up, the image of a good fighter being substantiate in a devalued opposition with the feminity: „the image of women is seen as fundamental element in the definition of a soldier's identity, functioning as a referential «other». Besides the masculine

[1] Johanna Valenius, *Gender mainstreaming in ESDP missions*, Chaillot Paper no. 101, European Union Institute for Security Studies, May 2007, p. 12.

[2] Francis Fukuyama, in a 1998 article, "Women and the Evolution of World Politics", published in „Foreign Affairs", basing his points on evidence drawn from biological studies, make a parallel between the chimpanzees and human race: "female chimps have relationships; male chimps practice realpolitik", and what results from this similarity is the conclusion that men (human males) will always dominate the politics; in the Fukuiama's vision, in an ideal world, women participation in decision-making it would be possible and wishful, but in the real world this kind of participation would end in a failure: the "macho cultures" of Asia, Africa and the Middle East would take over the West (F. Fukuyama, "Women and the Evolution of World Politics", *Foreign Affairs*, vol. 77, no. 5, September/October 1998, pp. 33 – 41).

models of the «hero», the «buddy» or the «tough man», soldiers are frequently exposed to negative images of women or homosexuals, used to represent the weak or inefficient qualities of the recruit"[3].

Secondly, in military conflicts, frequently, women are treated as sexual objects, rape and sexual exploitation/the forced prostitution being the main aspects of this relation. Rape is a constant aspect in wars, starting with religious ones, in the Middle Ages, and finishing with the contemporary ones, and it's main function is to create a state of terror between the enemies: „the very maleness of the military – the brute power of weaponry exclusive to their hands, the spiritual bonding of men at arms, the manly discipline of orders given and orders obeyed, the simple logic of the hierarchical command – confirms for men what they long suspect, that women are peripheral, irrelevant to the world that counts, passive spectators to the action in the center ring[…]. But rape in warfare has a military effect as well as an impulse. And the effect is indubitably one of intimidation and demoralization for the victims' side"[4].

At the same time, as Cynthia Enloe [5] emphasizes, prostitution itself became a "militarized" activity, in the war zones or near the military bases from Asia, Africa and Europe, where foreign soldiers are deployed. Otherwise, this phenomenon is also reported by the international organizations for human rights. In an annual report from 2010, elaborated for *Peacewomen Organization*, Jelena Prosevski[6], referring to the situation from Kosovo and Bosnia-Herzegovina, draws the attention on the fact that the "boom" on the women trafficking market was determined, mainly, by an increase of solicitations, explained by the presence of the peacekeeping forces. More than that, there were situations when representatives from these forces were directly involved in women trafficking, so that the author talks about a conflict reconfiguration: „this conflict in Bosnia and Kosovo is no longer along ethnic divisions, but it is an international gender conflict. Specifically, from a perspective of human trafficking, the conflict is mostly between men: on the one side, there are the traffickers (local and international, including peacekeepers), heavily financed by international peacekeeping personnel and most by women and, on the other side, there are the victims of trafficking, who, in the Balkans, tend to originate from the Ukraine, Moldova, Romania, Russia and the former Yugoslav republics"[7].

Therefore, for a long time, we can talk about an almost complete masculinization of the public discourse about security, men being situated on the side of state power and war, meanwhile women have a prevalent image as victims or objects of the war. Thus, we can talk not about a difference, but rather an hierarchy, because gender is used in a manner which justifies the fact that woman, "civilian" and "peaceful", is inferior to the warrior man, when we talk about security.

Still a few decades ago, women rights organizations took attitude against this way to use gender as a power relation, which made women' „voices" to be generally ignored when decisions about how to launch a military attack, how to manage a military conflict or regarding to the post-conflict actions, making them only "collateral victims" or passive spectators in the International Relations arena. Under the pressure of these organizations, at the international level, some conventions and resolutions were adopted, in order to integrate

[3] Helena Carreiras, *Gender and the Military: Women in the Armed Forces of Western Democracies*, Routledge, New York, 2006, p. 43.
[4] Susan Brownmiller, *Against Our Will. Men, Women and Rape*, Bantam Books, New York, 1976, pp. 25 – 26.
[5] Cynthia Enloe, *Maneuvers: The International Politics of Militarizing Women's Lives*, University of California Press, Berkeley and Los Angeles, California, 2000.
[6] Jelena Prosevski, *Gender Based Violence and Peacekeepers in Bosnia-Herzegovina and Kosovo*, 2010, http://www.peacewomen.org/assets/file/Resources/Academic/jelena_prosevski_writing__sample-gender_and_peacekeeping.pdf, accessed at 04.08.2014.
[7] Jelena Prosevski, *Op.cit.*, p. 2.

the gender perspective in various aspects related to the military operations and to the situation in the war zones.

2. International organizations approaches regarding gender mainstreaming in the security policies

2.1. United Nations Organization

As it is mentioned in the end of the previous chapter, as consequence of the women rights organizations actions, "the United Nations started to pay more attention to the roles of women in conflicts and peace processes" [8]. An important moment of this gender inclusion process on the United Nations agenda is represented by the 4th Word Conference for Women, in 1995, when a comprehensive action plan was adopted, known as "The Beijing Platform". In the document, to the point E (*Women and Armed Conflict*) of the Chapter IV (*Strategic Objectives and Actions*) is specified: „While entire communities suffer the consequences of armed conflict and terrorism, women and girls are particularly affected because of their status in society and their sex. […] The impact of violence against women and violation of the human rights of women in such situations is experienced by women of all ages, who suffer displacement, loss of home and prosperity, loss of involuntary disappearance of close relatives, poverty and family separation and disintegration, and who are victims of acts of murder, terrorism, torture, involuntary disappearance, sexual slavery, rape, sexual abuse and forced pregnancy […]"[9]. Also, the document contains a number of recommendations directed both to governments and to regional and international intergovernmental institutions, regarding the measures that should be taken in order to diminish this negative impact of military conflicts on women's lives. Most of these recommendations refer, on the one hand, to the necessity to better integrate women to the all decision-make levels in the peace-making processes, and, on the other hand, to the necessity that governments increase their efforts to transform the military resources development efforts and the related industries in a peaceful way of action, as distinct objective of national security politics.

Another important moment of the United Nations efforts is represented by the adoption, in 2000, by the UN Security Council, of the Resolution 1325, *Women, Peace and Security*. Recognizing „the urgent need to mainstream a gender perspective into peacekeeping operations"[10], as well as the fact that „an understanding of the impact of armed conflict on women and girls, effective institutional arrangements to guarantee their protection and full participation in the peace process can significantly contribute to the maintenance and promotion of international peace and security"[11], the Resolution „urges Member States to ensure increased representation of women at all decision-making levels in national, regional and international institutions and mechanisms for the prevention, management, and resolution of conflict"[12].

This document, as well as all that preceded it[13], appeared in a particular context: "war rapes and other kinds of sexual violence against women in the Yugoslavian and Rwandan

---

[8] Johanna Valenius, *Op. cit*., p. 15.

[9] *Beijing Declaration and Platform for Action, Fourth World Conference on Women*, 15 September 1995, A/CONF.177/20 (1995) and A/CONF.177/20/Add.1 (1995), http://www1.umn.edu/humanrts/instree/e5dplw.htm, accessed at 05.08. 2014.

[10] *UN Security Council Resolution 1325 (2000*), p. 2, http://www.unhcr.org/refworld/docid/3b00f4672e.html, accessed at 05.08.2014.

[11] *Idem.*

[12] *Idem.*

[13] *Windhoek Declaration* and *Namibia Plan of Action on Mainstreaming a Gender Perspective in Multidimensional Peace Support Operations*, both elaborated in 2000 and cited in the 1325 Resolution's Preamble.

wars received worldwide attention. For the first time, it was recognized that the rape of women in armed conflicts was an organized activity, even a method of warfare. Until then, war rapes were considered to just be an unavoidable side effect of armed conflicts […]."[14]

This context explains, in a good measure, the fact that many Resolution's stipulations refer to the women as military conflict victims, recognizing the necessity „for specialized training for all peacekeeping personnel on the protection, special needs and human rights of women and children in conflict situations".[15]

On the one hand, it is obvious that the UN Resolution 1325 offered to the international community a legal background which putted in the first place the gender issues in military conflicts, facilitating „formal recognition of women's rights in conflict and war situations and served to promote formal opportunities for dialogue between and among member states"[16].

On the other hand, there are many critical opinions regarding the Resolution, in these more than 10 years from its adoption.

First, there are authors who consider that the Resolution only transforms women in a discourse subject, ignoring the profound gender issues involved in the conflict situations: „women are «added» to the peace building discourse and power relations are left unexamined"[17].

Secondly, the critical points of view come from the researchers who find some significant differences between the Resolution's stipulations and the way in which these are implemented in the military operations. These gaps are explained, on the one hand, by the lack of a clear understanding about what gender mainstreaming in military operations really means: "in spite of pre-deployment training on gender issues, very few people actually know what mainstreaming gender entails in their area of responsibilities even if those people were committed to mainstreaming a gender perspective. This was an impression that the researchers also got when conducting the interviews with EUFOR, EUPM and EUSR officials"[18] On the other hand, "the resources, both in terms of money and staff, devoted to gender issues have been insufficient to meet the goals set by UN itself"[19].

On the basis of the Resolution 1325 and after 5 years after its adoption, the UN Security Council promoted the Resolution 1820, document considered as inner part of the UNSCR 1325 implementation process. In the new resolution, starting from the „deep concern that, despite its repeated condemnation of violence against women and children in situations of armed conflict, and despite its calls addressed to all parties to armed conflict for the cessation of such acts with immediate effect, such acts continue to occur, and in some situations have become systematic and widespread, reaching appalling levels of brutality"[20], the UN Security Council „notes that rape and other forms of sexual violence can constitute a war crime, a crime against humanity, or a constitutive act with respect to genocide"[21] and underline the necessity that these forms of sexual violence to be excluded from the amnesty, stressing, in this way, the gravity associated with this kind of acts, but, also, the need to find new and more concrete ways to punish it than a simple formal condemnation.

---

[14] Johanna Valenius, *Op. cit*., p. 15.
[15] *UN Security Council Resolution 1325* (2000), p. 2, http://www.unhcr.org/refworld/docid/3b00f4672e.html, accessed at 05.08. 2014.
[16] Heidi Hudson, *When Feminist Theory meets Peace Building Policy: Implications of Gender Mainstreaming and National Action Plans*, 2009, p. 3, http://www.allacademic.com//meta/ p_mla_apa_research_citation/3/1/3/9/0/pages313900/ p313900-1.php, accessed at 06.08 2014.
[17] *Ibid*, p. 1.
[18] Johanna Valenius, *Op. cit*., p. 16.
[19] Sandra Windworth (2004), apud Johanna Valenius, *Op. cit*., p. 16.
[20] *UN Security Council Resolution 1820*, p. 3, http://www.state.gov/documents/organization/106577.pdf, accessed at 07.08. 2014.
[21] *Idem*.

This series of Security Council resolutions ends in 2013 with UNSCR 2106 and 2122. In the Resolution 2016 regarding the sexual violence in conflicts, unlike other resolutions relating to this type of violence, one of the main topics was the effective women's participation: "in contrast to the earlier resolutions on sexual violence in conflict […] in which the emphasis on women's empowerment and gender equality was notably weak, Resolution 2016 includes some language on these issues, for instance pp. 1 «stresses women's participation as essential to any prevention and protection response»"[22]. Also, in its adoption process, there were some civil society speakers who underline the fact that the main causes of sexual violence consist "in unequal gender power relations and the perception of woman as man's inferior"[23]. After a few months, in October 2013, the adoption of Resolution 2122, "which is primarily focused on increasing women's participation in conflict prevention and all areas of peace processes"[24] brought to the front "the need to address the full scope of women's human rights violation rather than sexual and gender based violence alone"[25], expanding the future discussion area.

Therefore, in the nearly 15 years between the adoption of the Resolution 1325 and the latest UN resolutions on gender issues in the context of global security, it may be noticed a passage from a speech focused on the image of women as victims of sexual or other kind of abuse in the context of military conflicts, to a more nuanced one, which includes aspects related to the need to involve women in processes regarding their own security. It is, also, notable the growing number of explicit public positions questioning the deep causes of violence against women in situations of armed conflict, placing them in the systemic gender inequalities and the stereotypical mentalities that make women "second-class" citizens of the world, but these positions come mainly from the civil society and less from the state or international bodies and institutions.

2.2. NATO

One of the most important structures involved in the implementation of UNSCR 1325 and all another related ones is NATO, as military-political organization with ambtious declared objectives in promoting international security.

According to the information contained in one document posted on the official website of the organization[26], about the UNSCR 1325 implementation, NATO involvement in the promotion of its stipulations and hence in their implementation within its own policy was officially decided in the Euro-Atlantic Partnership Council meeting, held in December 2007, while guidelines for integrating this resolution in NATO Command Structure were established in the strategic commands, during 2009.

The same document describes NATO's available resources to implement Resolution 1325, and one of the most important one is the NATO Committee on Gender Perspectives, which have a main and explicit goal to advise "NATO leadership and Member Nations on gender related issues in order to enhance organizational effectiveness in support of Alliance

[22] Security Council Debate on Sexual Violence in Conflict, June 2013, http://www.peacewomen.org/security_council_monitor/debate-watch/all-debates/62/security-council-open-debate-on-sexual-violence-in-conflict-june-2013-security-council-resolution-2016, accessed at 07.08.2014.
[23] *Idem.*
[24] Security Council Open Debate on Women, Peace & Security, 18 October 2013, http://www.peacewomen.org/security_council_monitor/debate-watch/all-debates/70/security-council-open-debate-on-women-peace-and-security-october-2013 , accessed at 07.08. 2014.
[25] *Idem.*
[26] *Women, peace and security*. *NATO's implementation of UNSCR 1325*, http://www.nato.int/cps/en/natolive/topics_56984.htm, accessed at 08.08.2014.

objectives and priorities, including the implementation of relevant United Nations Security Council Resolutions (UNSCRs)"[27].

The importance attached to these UN Security Council Resolutions by the command structures of the Alliance was highlighted, also, during the last two NATO Summits[28], in Lisbon and Chicago. In Lisbon Summit Declaration, at the 7th point, it states the following: "We welcome the 10th Anniversary of UNSCR 1325 on Women, Peace and Security. Guided by the Policy that we developed together with our Partners in the Euro Atlantic Partnership Council, we have already taken significant steps to implement it and its related Resolutions. We have today endorsed an Action Plan to mainstream the provisions of UNSCR 1325 into our current and future crisis management and operational planning, into Alliance training and doctrine, and into all relevant aspects of the Alliance's tasks. We are committed to the implementation of this Policy and Action Plan as an integral part of our work to improve the Alliance's effectiveness, and today we endorsed recommendations to this end. We have tasked the Council to provide a progress report to our Foreign Ministers in December 2011 and at the next Summit"[29].

Two years latter, the 16th point of the Chicago Summit Declaration 2012 recognized the fact that "widespread sexual and gender-based violence, in conflict situations, the lack of effective institutional arrangements to protect women, and the continued under-representation of women in peace processes, remain serious impediments to building sustainable peace" and reaffirmed the fact that "we remain committed to the full implementation of United Nations Security Council Resolution (UNSCR) 1325 on Women, Peace and Security […]"[30].

As it can be noted above, and as Cynthia Cokburn, one of the US feminist antimilitaristic movement representatives emphasized, "NATO has adopted UNSC Resolution 1325 with an energy that could easily pass for enthusiasm"[31]. However, this enthusiasm is not always appreciated as a positive aspect in relation to the initial objectives of the Resolution 1325. Beyond all these actions, as Cynthia Cokburn pointed out, there are some contradictions between UNSCR 1325 provisions and the NATO policy for the implementation of these provisions. The first of these, as the author believes, stems from the fact that "UNSC Resolution 1325 does *not* in fact call for more women in armies. It urges, in rather careful terms, an expansion of «the role and contribution of women in United-Nations field-based operations, and especially among military observers, civilian police, human rights and humanitarian personnel» […] It has picked up the ball of gender equality thrown into play by feminists and is running with it for its own objectives"[32].

Secondly, according to the same author, "NATO is a militarist organization; yet the intention of 1325 is antimilitarist; yet its wording and provisions leave it co-optable by militarism"[33]. This co-optation is facilitated, in Cockburn's opinion, by the different meanings of the term "security": "in the concept of «women security», we gave «human security» gender specificity. This was, for feminists, the meaning of the word in the title of the

[27] NATO Committee on Gender Perspectives, http://www.nato.int/cps/en/natolive/topics_50327.htm, accessed at 08.08.2014.
[28] When the present paper was elaborated, the NATO Summit 2014 was just at the beginning, so there are no official documents available.
[29] *Lisbon Summit Declaration* (issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Lisbon), http://www.nato.int/cps/en/natolive/official_texts_68828.htm, accessed at 08.08.2014.
[30] *Chicago Summit Declaration 2012*, http://www.nato.int/chicago2012/ , accessed at 08.08.2014.
[31] Cynthia Cokburn, *Snagged On The Contradiction: NATO, UNSC Resolution 1325, and Feminist Responses*, „No to War No to NATO" Conference Paper, Dublin, 15 – 17 of April 2011, p. 3, http://www.wloe.org/fileadmin/Files-EN/PDF/no_to_nato/women_nato_2011/NATO1325.pdf, accessed at 09.08.2014.
[32] *Ibid*., p. 6.
[33] *Idem.*

Resolution: Women, Peace and Security. The ideal of «security» can however too readily be manipulated by an organization such as NATO that, however it describes security in words, manifests it in action as meaning the militarization of society and a readiness to fight wars"[34]. The third aspect highlighted by Cynthia Cokburn consists in the fact that "some women who were involved in the movement to obtain Resolution 1325 were self-critical afterwards on the grounds that they had failed at any point to express *an explicit critique of men, masculinity and patriarchy* in relation to militarism, militarization and war", observation which still remain available, despite the fact that are some attempts to bring this topic to discussion, when the UNSCRs 2106 and 2122 were adopted, as it is shown above.

From a total different point of view, and despite all these criticisms, some NATO actions dedicated women integration in military forces are positively appreciated, especially in war zones where women situation in society, as well as cultural habits make the relationship between the local population and military forces problematic. Thus, Stefanie Babst, Acting NATO Assistant Secretary, listed in the speech which she held during the Conference on Women, Peace and Security – the Afghan View – Talinn, 2010[35], some of the positive effects of gender mainstreaming measures in ISAF operations in Afghanistan. First, highlights Babst, "we now provide gender awareness training to the civilian and military teams before they deploy on operations. This provides them, for example, with an understanding why in matters to take a different approach when searching an Afghan woman or an Afghan man, or why male ISAF personnel should avoid looking an Afghan woman in the face" [36]. Secondly, "female soldiers can conduct searches on Afghan women at checkpoints, without causing offense. Female military doctors and nurses can run clinics where women will more easily go for treatment"[37]. But, despite all these positive aspects, and even if we ignore the antimilitaristic vision, it still remains questionable how this approach could be integrated in a gender mainstreaming perspective, transformative by definition, as long as these actions seem rather dedicated practical purposes, to ensure the success of the military mission itself and only secondary to improve the Afghan women lives.

Conclusions

Nowadays, even the female presence in the modern armed forces and in some institutional entities with a role in developing and promoting policies and strategies in the field of security is improved, a number of stereotypes about the role of each gender category in these processes continue to persist. According to these stereotypical ways in defining men and women roles regarding the security issues, women are often perceived as a referential used to build the men identities as active "actors" in the war and security policy scene, or as mere victims of sexual or another kind of abuses in the conflict zones. Without denying the fact that the war affects women in a particular way, but starting at this kind of considerations, as a matter of fact, UN adopted an entire series of resolutions on women, peace and security, starting with the most important one, UNSCR 1325, in 2000. This particular resolution, drafted by women rights organizations, and adopted under their pressure, draw attention to the impact of armed conflict specifically on women, but in the same time, getting women recognized as active actors, capable of contribution to the end of these conflicts, to achieve

[34] *Ibid*., p. 7.
[35] Stefanie Babst, *Role and Experience of International Organizations in implementation of UNSCR 1325 in Afghanistan*, remarks at the Conference on Women, Peace and Security – the Afghan View – Talinn, Estonia, 2010, http://www.nato.int/cps/en/SID-D2865947-5CE90518/natolive/opinions_68078.htm?selectedLocale=en, accessed at 09.08.2014.
[36] *Idem.*
[37] *Idem.*

peace and redefine security. Initially, this redefinition of security was thinking in terms of "women security", as particular form of "human security", but according to some feminist authors, because the term "security" itself supposes multiple connotations, some discrepancies appeared between the initial purposes of the UNSCR 1325 and the concrete ways of its implementation, especially when we referred at NATO, which seems to understand this implementation, as these authors highlighted, mainly as a way to increase the number of the military women in the conflict areas and the chances for military actions to end successfully. Despite these critiques, it seems that some aspects related with NATO's actions dedicated to gender mainstreaming in military operations are favorably appreciated, especially regarding Afghanistan, where the presence of military women in ISAF Forces made, in a lot of circumstances, the Afghan women situation less difficult as usual.

Finally, it has to be mentioned the fact that the adoption of the last two UN Resolutions regarding Women, Peace and Security, in 2013, has offered the opportunity for some NGOs to publicly express their concern about the deep, systemic causes of the violence against women. Even if these public positions are sporadic and adopted mainly by the NGOs and less by the representatives of the international institutions, it could be considered as a promising start for a reconceptualization of the term "women security" by questioning all these aspects of systemic violence against women, generated by a patriarchal way to see gender relations as power relations.

BIBLIOGRAPHY:

1. BABST, Stefanie, *Role and Experience of International Organizations in implementation of UNSCR 1325 in Afghanistan*, remarks at the Conference on Women, Peace and Security – the Afghan View – Talinn, Estonia, 2010, http://www.nato.int/cps/en/SID-D2865947-5CE90518/natolive/opinions_68078.htm?selectedLocale=en.
2. BROWNMILLER, Susan, *Against Our Will. Men, Women and Rape*, Bantam Books, New York, 1976.
3. CARREIRAS, Helena, *Gender and the Military: Women in the Armed Forces of Western Democracies*, Routledge, New York, 2006.
4. COKBURN, Cynthia, *Snagged On the Contradiction: NATO, UNSC Resolution 1325, and Feminist Responses*, „No to War No to NATO" Conference Paper, Dublin, 15 – 17 of April 2011, http://www.wloe.org/fileadmin/Files-EN/PDF/no_to_nato/women_nato_2011/NATO1325.pdf, accessed at 09.08.2014.
5. ENLOE, Cynthia, *Maneuvers: The International Politics of Militarizing Women's Lives*, University of California Press, Berkeley and Los Angeles, California, 2000.
6. FUKUYIAMA, Francis, *Women and the Evolution of World Politics*, Foreign Affairs, vol. 77, no. 5, September/October, 1998, pp. 33 – 41.
7. HUDSON, Heidi, *When Feminist Theory meets Peace Building Policy: Implications of Gender Mainstreaming and National Action Plans*, 2009, http://www.allacademic.com//meta/p_mla_apa_research_citation/3/1/3/9/0/pages313900/ p313900-1.php.
8. PROSEVSKI, Jelena, *Gender Based Violence and Peacekeepers in Bosnia-Herzegovina and Kosovo*, 2010, http://www.peacewomen.org/assets/file/Resources/Academic /jelena_prosevski_writing__sample-gender _and_peacekeeping.pdf.
9. VALENIUS, Johanna, *Gender mainstreaming in ESDP missions*, Chaillot Paper no. 101, European Union Institute for Security Studies, May, 2007, p. 12.

10. *Beijing Declaration and Platform for Action, Fourth World Conference on Women*, 15 September 1995, A/CONF.177/20 (1995) and A/CONF.177/20/Add.1 (1995), http://www1.umn.edu/humanrts/instree/e5dplw.htm.
11. *Lisbon Summit Declaration* (issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Lisbon), http://www.nato.int/cps/en/natolive/official_texts_68828.htm.
12. *UN Security Council Resolution 1325 (2000*), p. 2, http://www.unhcr.org/refworld/docid/3b00f4672e.html.
13. *UN Security Council Resolution 1820*, p. 3, http://www.state.gov/documents/organization/106577.pdf.
14. *Women, peace and security*. *NATO's implementation of UNSCR 1325*, http://www.nato.int/cps/en/natolive/topics_56984.htm, accessed at 08.08.2014.
15. Security Council Debate on Sexual Violence in Conflict, June 2013, http://www.peacewomen.org/security_council_monitor/debate-watch/all-debates/62/security-council-open-debate-on-sexual-violence-in-conflict-june-2013-security-council-resolution-2016.
16. Security Council Open Debate on Women, Peace & Security, 18 October 2013, at http://www.peacewomen.org/security_council_monitor/debate-watch/all-debates/70/security-council-open-debate-on-women-peace-and-security-october-2013.
17. NATO Committee on Gender Perspectives, http://www.nato.int/cps/en/natolive/topics_50327.htm.
18. Chicago Summit Declaration 2012, http://www.nato.int/chicago2012/.

ORGANIZED CRIME, TRAFFICKING IN DRUGS AND ITS CORRELATIONS WITH THE SECURITY ENVIRONMENT

Sorin OPREA
Quaestor, Director of National Antidrug Agency, Romania.

Abstract: *With a constantly increasing trend, drug demand provides an attractive and extremely profitable market for criminal organizations operating in the field of trafficking in drugs. At the same time, money resulted from trafficking in drugs at global level represents a vital and indispensable segment for the whole monetary system, amounting 6% of the total global commercial exchanges, similarly to oil market.*

At global level, the two primordial components of trafficking in drugs, which are the cocaine transportation route coming from Latin America and heroin transportation route coming from Afghanistan, can be viewed at the same time as two black money flows, but also as social, political and economic turbulences for the transit zones.

This is explained by the fact that, on the one hand, these countries' budgets are much smaller than the value of drug flows, that is the "black money" that crosses their territories, and, on the other hand, by the geopolitical influence that trafficking in drugs exerts at global level.

Key words*: trafficking, drugs, crime, money laundering, globalization*

1. Globalization: "benefits" and "prejudices" to mankind

Globalization has considerably contributed to developing the modern society, by bringing a lot of incomes, most of which belonging to business environment and especially to trade. Thus, due to globalization, today the free movement of goods is possible, we live in a world with almost instantaneous communication, we travel much easier, at much lower costs. The dark side of globalization is represented by the increasing organized transnational crime and terrorism which, corroborated with the development of information and communication new technologies, has led to a more rapid propagation of drug phenomenon at global level with all its sides: trafficking, use, production.

We can state that today drug illicit trafficking and use can no more be limited to a certain geographical or cultural zone, as the trafficking methods, consumption models and production technologies can no more be assigned to certain patterns already known.

Criminal organizations are more and more powerful and diverse; they get usually involved in systematic ways of cooperation meant to dissimulate their criminal activities.

With a constantly increasing trend, drug demand provides an attractive and extremely profitable market for such criminal organizations. By benefiting from the high mobility provided by the new communicational age and the possibility to use legal trade in order to conceal illicit drugs, they use the global banking system to accumulated, move and launder the profits obtained from their illegal activities, by being more and more ingenious in their smuggling methods.

According to the "Estimation of illicit financial flows resulted from drug trafficking and other organized transnational crime activities" research drawn up by UNODC, in 2009 trafficking in drug produced 870 billion of dollars per year, amounting during the first decade

of the new millennium 1.5% of the GDP[1].

On the other hand, analyses have shown that approximately 10-15% of drugs are intercepted and the rate of seized money is smaller than 0.5% of the real value[2]. This leads to the conclusion that the remaining money coming from drug trafficking at global level goes freely to the market and becomes part of the money flow used at global level.

In this context, banks without scruples practicing financial operations at a wide level beyond their capacity to assume their responsibility for their obligations, strive to ensure their cash flows by absorbing huge amounts of money coming from criminal activities, most of which coming from drug trafficking.

According to Antonio Cost, ex Sub secretary General of ONU[3], during the 2008-2009 global crisis approximately 352 million of narco-dollars were introduced in important banks at global level in order to avoid the lack of cash flow. Later on, this money was used for loans between banks. This is not surprising at all, because according to IMF, important American and European banks lost over 1 trillion of dollars due to "toxic" assets between January 2007-December 2009 when over 200 high hypothecation companies and other financial institutions went bankrupt[4].

2. Money laundering coming from drug trafficking

The relation between banking system and mafia started in the '60s and '70s, when mafia was manipulating big amounts of money but the international criminality level was small. It included the most part of Italy, North America and other affiliations. Then, when the borders progressively opened through communication and business relationships, at the end of '70s and beginning of the '80s, organized crime originated outside Italy started to use banking system in order to transfer assets or to move money throughout the world.

At the beginning of the '80s within the G7 meetings a key document was drawn up to create the first and more important institution fighting against money laundering: Financial Action Task Force (FATF). FATF started its activity with specialized recommendations. These recommendations started to be applied progressively, which determined a significant decreasing of black money recycling through the banking system.

On the other hand, at international level there a ONU Treaty according to which laundering of money coming from drug trafficking is considered a crime punishable at global level. Thus, according to ONU Convention in the field of drugs, concealing and dissimulating the nature, source or possession of proceeds from illegal activities, such as drug trafficking is a crime[5].

During 2002-2003, when the economic crisis hit for the first time, the banking system was also affected. At this time, criminal assets began to be infiltrated in the banking system, and this phenomenon spread enormously due to globalization. In this context, anti-money laundering controls, which worked very effectively in the 1990s in Europe and North America decreased significantly in a number of offshore jurisdictions, which led to the beginning of a new penetration cycle of the dirty money in the banking system.

The lack of liquidity associated with the banking crisis, banks' reluctance to lend

---

[1] United Nations Office on Drugs and Crime (UNODC), *Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes - Research Report*, October 2011, p. 7.

[2] Victor Ivanov, *Drug Trafficking and the Financial Crisis*, Executive Intelligence Review, Volume 38, Number 47, 2 December 2011.

[3] *Idem.*

[4] Reuters, *FACTBOX-U.S., European bank writedowns, credit losses*, 5 November 2009, www.reuters.com/article/2009/11/05/banks-writedowns-losses-idCNL554155620091105?rpc=44.

[5] Petre Albu, *Crima organizată în perioada de tranziţie – o ameninţare majoră la adresa securităţii internaţionale*, Editura Ministerului Internelor şi Reformei Administrative, 2007, p. 48.

money to one another provided a great opportunity for criminal organizations, which developed a great financial power due to the possession of cash that could not be "washed" in previous years through the banking system. Thus, periods of economic crisis made visible the lack of cash flows. However, the existing financial system, which operates by using a large number of instruments designed to "inflate" the so called "financial bubble", could not exist anymore without introducing the black money.

This analysis is confirmed entirely by the expertise presented in the research report published by the United Nations Office for Drugs and Crime "Estimating illicit financial flows resulting from drug trafficking and other transnational organized crime activities"[6].

The report states that black money can easily enter into the legal financial flows; at the same time "investments" with such money seriously disrupt the real economy and substantially impede growth. The report estimates that the total flow of black money of organized crime amounts to 870 billion of dollars per year, amounting for the first decade of the new millennium, an amount of 1.5% of world GDP.

According to this document, no less than 70% of this money is laundered through financial institutions. The most profitable sector of the "black" economy is the illicit drug trade, which is minimum half from the global criminal flows[7]. The report estimates that the economic damage caused by drug trafficking is double or triple compared to the value of the drugs.

Thus, while the cocaine market in the USA is estimated at $ 35 billion and that of heroin and other drugs at $ 15 billion, the direct damage produced to the United States economy, because of the drugs, is estimated at around 150 billion dollars.

Given that similar drug markets are active in the European Union and China as trading and economic partners with the United States, this has an adverse effect on a large scale, which is reproduced in the form of negative synergies. Because Europe is the largest market for heroin in Afghanistan, and in Latin America is half the market for cocaine, there are big chances that the major countries economies of the world to collapse much faster. Black drug money simply lead to an exhausted economy development.

3. Wachovia Bank case

To illustrate the manner in which the banking system relies on money coming from drug trafficking, we present the case of Wachovia Bank, whose investigations into financial transactions, conducted between 2004 and 2007, were widely analyzed in the international media. According to the United States Justice Department, Wachovia Bank has recycled 378.4 billion dollars, over a period of three years[8].

Thus, in the early 2010, the Bank signed an agreement settled out with the United States regulating authorities, paying approximately 150 million dollars in exchange for the withdrawal of accusations about assistance in money laundering.

This led to a 22 months investigation, carried out by officers of the United States Anti-Drug Agency, the Mexican drug cartels have made transactions through the bank using electronic transfers, traveling checks and cash.

According to federal prosecutor Jeffrey Sloman, there was a “blatant disregard for our laws coming from Wachovia Bank that gave international cocaine cartels a virtual white card to finance the money laundering operations regarding the proceeds from the sale of drugs”[9].

---

[6] UNODC, *op. cit.*, October 2011.
[7] *Ibidem,* p. 10.
[8] Ed Vulliamy, *How a big US bank laundered billions from Mexico’s murderous drug gangs*, 3 April 2011, www.theguardian.com/world/2011/apr/03/us-bank-mexico-drug-gangs.
[9] Victor Ivanov, *op. cit.*, 2 December 2011.

The most unfortunate thing was that the bank was found guilty of transferring 378.4 billion dollars (an amount equal to one-third of the Mexican GDP) from the so-called exchange offices in Mexico. There are other similar cases in which the banks have not notified the financial information about such operations.

In addition to the Wachovia case, US anti-drug police officers also reported other criminal transactions regarding another large bank, the Bank of America. In one of the cases there were traced transactions related to the sale of 22 tons of cocaine, and in another one the transactions were linked to the sale of about 10 tons of cocaine.

Likewise, other banks also came under suspicion of illegal transactions and were fined, including American Express Bank and HSBC.

The tragedy of Wachovia case is that those who were responsible for laundering money resulted from Mexican drugs were released without any punishment. In the case of Wachovia Bank, it has been very clear that people have not necessarily entered a branch of the bank somewhere in New York with a suitcase full of money, but on the contrary, the submission was made in Mexico or in one of the Central American countries, and then the money found their way to the Wachovia Bank in the USA.

Behind this phenomenon there is the very nature of the current global financial system, being quite evident that different types of surrogate money or various derivatives or secure bonds have had a certain role in the so-called "financial bubble".

However, almost no one pays attention to such a paradox: while the economy is weak and the crisis escalated, the banks managed to obtain liquidity and manage liabilities. On the other hand, studies[10] have shown that the continued lack of cash flow and attempts to stay afloat during a crisis, promote not only tolerance for black money, but also an attitude encouraging the availability of this type of money.

Moreover, for example, the possibility of continuing need for liquid coatings acts in many respects, as an on-going spring between financial markets and economic demand for the production of drugs.

Money from drug trafficking worldwide is actually not only valuable items, but as donors of liquidity, which are increasingly rare, is a vital and indispensable segment of the entire monetary system.

4. Flows of the drug crime and security of the transit countries

Although it is estimated to be approximately the same size as the oil market (6% of total world trade), narcotics market impact is not considered by economists and politicians. Therefore, the development of appropriate control policies should be based on a deep understanding of the specific drug trafficking worldwide.

So far, unfortunately, the drug policies were dominated by local efforts or, at best, regional or interregional efforts. To develop appropriate solutions and to understand better what is happening, a better approach is needed regarding the flow of drugs worldwide. According to the experts, the primary ability of a drug flux is placed beyond the local and regional levels, which is located at the top of the pyramid flows drug crime globally.

[10] Thomas F. Huertas, *Crisis: Cause, Containment and Cure*, Palgrave MacMillan, 2011, pp. 30-50.

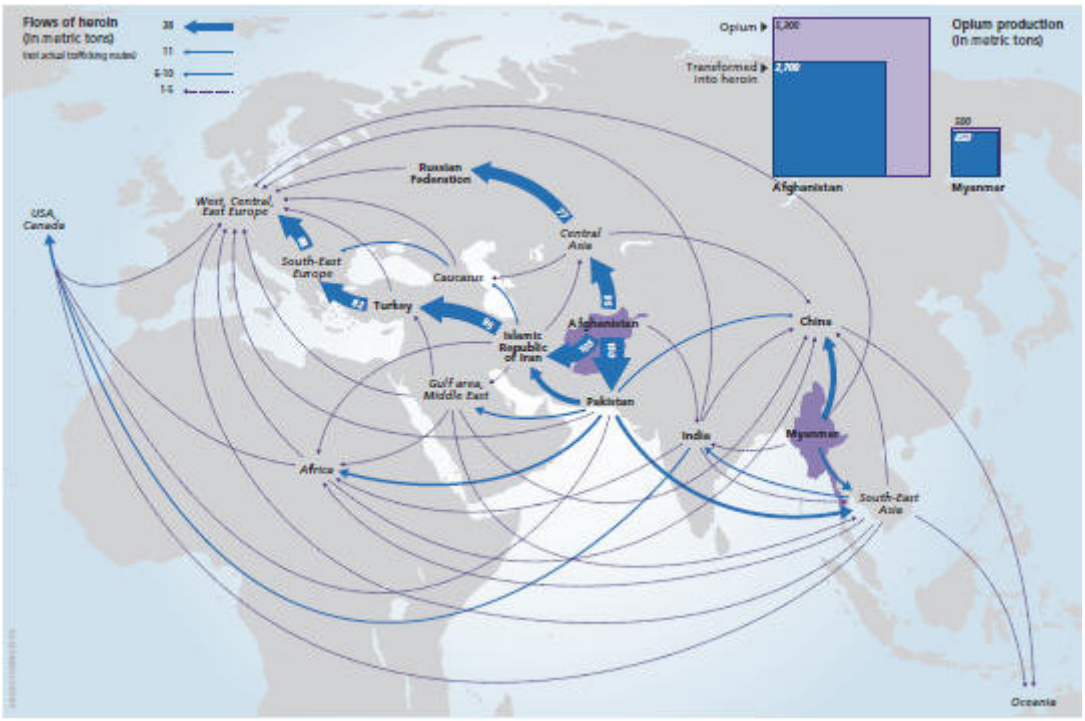


Figure no. 1. Routes used in heroin trafficking
Source: UNODC, World Drug Report 2010, Vienna, 2010

The structure of distribution of the proceeds of cocaine production worldwide, with total revenues in 2009 of approximately $ 84 billion, indicates the same structure. While the Andean coca farmers earned about $ 1 billion, most of the revenues of $ 35 billion were concentrated in the North America, with another $ 26 billion in Central Europe.

In North America and Europe, naturally, almost 80% of the revenues of the illicit trade in cocaine are washed[11], while only one-tenth of the proceeds from other regions are washed in the Caribbean.

Currently, there are two obvious components of global drug trafficking or rather two routes of drugs: the cocaine route from Latin America and the route of heroin from Afghanistan. The direction, intensity and extraordinary ability of these two components of drug trafficking require to be labeled, more specifically, as “flows”.

The devastating ability of these two drug streams is particularly noticeable if you look at the situation of the drug transit countries, where endless social and political turbulences are to be found. One explanation is that the budgets of these countries are less than two or three times the amount of drug that flows across the territories.

The budgets of Tajikistan and Kyrgyzstan, located on the Northern route of Afghan heroin, are often less than the financial capacity of the flow of drugs from Afghanistan, crossing their territory.

Unfortunately, the globalization of the drug trafficking and the emergence of global drug flows, sweeping everything in their path, have also become a common thing for the countries of the Balkan Peninsula. It is sufficient to note that Kosovo has become the focus point of drug trafficking in Europe, an epicenter where, on one hand, two drug streams crosses each other – cocaine from Africa and heroin from Turkey, and on the other hand, their transshipment occurs, oriented towards the EU.

According to UN estimations, approximately 50 tons of heroin annually transit the European center of cocaine and heroin distribution, with an annual transit profit of about 3

[11] UNODC, *World drug report 2009*, Vienna, 2009.

billion euros, twice the size of the budget of Kosovo[12]. The same trends are observed in the cocaine trafficking in Niger, Guinea Bissau and other African countries. Moreover, analysis of the global cocaine trafficking mainly denotes its orientation towards Europe, while hundreds of new transit routes from Latin America to Europe via West Africa have appeared.

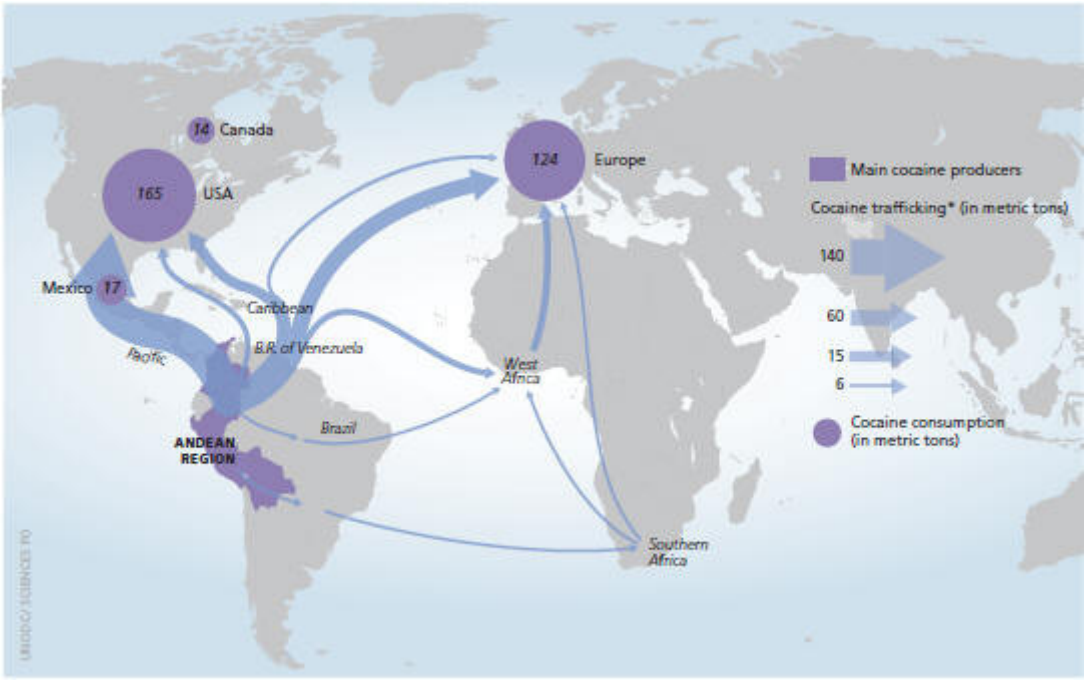


Figure no. 2. Routes used in cocaine trafficking
Source: UNODC, World Drug Report 2010, Vienna, 2010

In this context, drug trafficking has quickly become a dominant criminal geopolitical factor, one who has the financial resources, technology and important human resources and mobilized for a global political and economic reform. The most obviously examples of this are the civil war from Guinea Bissau, Mauritania and Niger, and the Ivory Coast. Drug trafficking has also contributed to the destabilization of the situation in the Arabian countries.

These destabilizing examples from the transit countries represent another drug trafficking problem of the global dimension. Only a comprehensive and integrated understanding of the nature and dynamics of these global drug flows will allow us to understand the essence of the threat posed by drug-related crime.

Conclusions

On the one hand there is a well-organized bank proper system, and the mafia and criminal organizations on the other. Between these two entities there are an army of bankers, financial advisers, estate agents, notaries, lawyers, and so on, which are part of the problem itself. Efforts are very small in an attempt to destroy them.

Countries, companies, governments must be able to break the link between the real criminals, those who got the weapons belt and bankers. In the financial institutions are people who are involved, not necessarily in money laundering, but the paper work, work needed to turn dirty money into legal money.

There should be built a strong relationships between governments leading to the establishment of a global anti-drug coalitions, in close cooperation with politicians,

[12] UNODC, *World drug report 2011*, Vienna, 2011, pp. 18-21 and 121-129.

economists and financiers, which would lead to combat international drug trafficking.

It is quite obvious that clear up "financial bubble" must be supported by eliminating drug production capabilities, based on renewable bioresources: coca and poppy bush as a primary source for obtaining drug money. Repressive measures only are not sufficient in drug trafficking.

The way in which global drug trafficking is to be eliminated is by reforming the existing economy and moving to an economy that excludes the use of black money and ensures continuous creation of clean liquid assets, i.e., to a development economy in which decisions are based on development projects and loans targeted on long terms.

BIBLIOGRAPHY:

1. ALBU, Petre, *Crima organizată în perioada de tranziţie – o ameninţare majoră la adresa securităţii internaţionale*, Editura Ministerului Internelor şi Reformei Administrative, 2007.
2. HUERTAS, Thomas F., *Crisis: Cause, Containment and Cure*, Palgrave MacMillan, 2011.
3. IVANOV, Victor, *Drug Trafficking and the Financial Crisis*, Executive Intelligence Review, Volume 38, Number 47, 2 December 2011.
4. MACHADO, Lia Osório, *Les mouvements d'argent et le trafic de drogue en Amazonie brésilienne*, Autrepart (8), 1998.
5. ŢONE, Cătălin şi alţii, *Drogurile şi crima organizată*, Editura Sitech, Craiova, 2009.
6. ŢONE, Cătălin, *Influenţa traficului de droguri asupra siguranţei naţionale*, Teză de doctorat susţinută la Universitatea Naţională de Apărare „Carol I", Bucureşti, 2011.
7. VULLIAMY, Ed, *How a big US bank laundered billions from Mexico's murderous drug gangs*, 3 April 2011, http://www.theguardian.com/world/2011/apr/03/us-bank-mexico-drug-gangs.
8. Reuters, *FACTBOX-U.S., European bank writedowns, credit losses*, 5 November 2009.
9. United Nations Office on Drugs and Crime (UNODC), *World drug report 2009*, Vienna, 2009.
10. UNODC, *World drug report 2010*, Vienna, 2010.
11. UNODC, *World drug report 2011*, Vienna, 2011.
12. UNODC, *World drug report 2013*, Vienna, 2013.
13. UNODC, *World drug report 2014*, Vienna, 2014.
14. UNODC, *Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes - Research Report*, 2011.
15. ***, *The Economic Impact of Illicit Drug Use on American Society, United States Department of Justice, 2011.*

EUROPEAN INSTITUTIONS INVOLVED IN THE FIGHT AGAINST SERIOUS FORMS OF CRIME

Octavian AMBROZIE
PhD, Lawyer within the Bar of Bucharest.
E-mail address: o.ambrozie@gmail.com

Abstract: *This article deals with the European Union institutions that fight against serious forms of crime, while highlighting how they provide support and coordinate the efforts of national authorities.*

Keywords*: serious forms of crime, European Institutions, EUROPOL, EUROJUST.*

Introduction

The European Union is an economic and political union consisting of 28 member states and supporting the free movement of people, goods, services and capital by means of its policies. Along with the movement of people of good faith, on the European Union territory, from one state to another, criminal elements move, as well.

In other words, aside from the benefits offered to all of us, by opening borders and the liberalization thereof, crime also took advantage. Therefore, criminals can move more easily and can transfer various goods much faster and easier.

Many physical and legislative barriers were removed from the European Union. However, in terms of criminal law, each Member State has its own regulation. This makes the procedures for cross-border crime investigations more difficult. Therefore, important time is lost and often communication between the states involved may be hampered.

To simplify these issues, especially the legislative ones, there were created a range of European institutions such as EUROPOL and EUROJUST. They also ensure coordination and cooperation for the fight against crime with a major impact on the European Union or the Member States, including in the case of serious crime.

Serious crime poses a grave threat to the security of every state in which it occurs, as well as substantial economic loss. For example, in the UK, 24 billion pounds are annually lost because of this scourge[1]. Another effect is that more and more people are becoming victims of criminal activities in the range of serious crime, some becoming drug addicts, others being trafficked or even victims of violent actions followed by death.

1. European instruments for fighting against serious crime

At EU level, with the increased freedom of movement, it was noticed that crime has acquired, in turn, an international spread, with criminals coming to act with greater ease across borders.

[1] Serious and Organised Crime Strategy Presented to Parliament by the Secretary of State for the Home Department by Command of Her Majesty, October 2013, p. 5, at the address https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/248645/Serious_and_Organised_Crime_Strategy.pdf.

Combating crime involves strengthening dialogue and action between the criminal justice authorities of Member States.[2] Consequently, the European Union has established a sole area of criminal justice, aside from institutions such as EUROPOL and EUROJUST which fight directly against serious crime.

The creation of the common space for criminal justice was possible due to specific tools for judicial cooperation in criminal matters.

Judicial cooperation in criminal matters is based on the principle of mutual recognition of judgments and judicial decisions by the Member States. It involves the correlation of national laws on the matter and the enactment of common minimum rules. The minimum rules mainly relate to the admissibility of evidence and the rights of crime victims, as well as of individuals subject to criminal procedures.[3]

1.1. Mutual Legal Assistance in Criminal Matters

Mutual Legal Assistance in Criminal Matters was introduced in 2000 by the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union. This Convention rules the support and effective cooperation between judicial, customs and police authorities in criminal matters.

With this tool, it is possible for a Member State to establish direct links with the judicial authorities in another Member State to carry out prosecution procedures. Moreover, it also allows for spontaneous exchange of information between EU Member states for certain crimes' investigation.

This is a useful tool that allows for major activities related to criminal matters, such as:

- providing the requesting state with property found in another Member State;
- temporary transfer to another Member State of a person detained in another state for the hearing of such person (only with the consent of the person concerned);
- hearing a witness or expert by video conference;
- delivery under surveillance on the territory of another Member State;
- undercover investigations;
- interception of communications.

The act governing mutual assistance in criminal matters came into force in 2005. Its entry into force created real preconditions and legislative tools to help in the fight against crime of any kind, including severe crime.

1.2. Mutual recognition of judgments in criminal matters

This is one of the key elements in the field of judicial cooperation in criminal matters because this instrument helps to avoid various difficulties that may arise in the enactment of criminal law as a result of difficulties due to legislative differences between Member States. Thus, we are not dealing with situations of double incrimination or situations where a penalty to be imposed pursuant to a final judgment given in a Member State is not observed in another Member State. In other words, an EU citizen who was sentenced as a result of the enforcement of criminal law in a Member State cannot go to another Member State to evade it.

1.3. The European Arrest Warrant

This was a welcomed tool as it replaced the old traditional system, introducing many beneficial rules such as limited grounds for refusal of execution, decision-making shifting

[2]http://europa.eu/legislation_summaries/justice_freedom_security/judicial_cooperation_in_criminal_matters/index_ro.htm.
[3] *Idem.*

from political to judicial authorities, the possibility to surrender nationals of the executing state and clear timeframes for carrying out each European Arrest Warrant[4].

1.4. Harmonisation of legislation

At European level, criminal law is not unique; however the European institutions have made a considerable effort, with beneficial effects to create joint standards. Thus, the deeds specific to severe crime are jointly defined by laws, while attempting at the same time to achieve a uniform level of punishment.

1.5. Procedural rights

At European level, the European legislative bodies have been trying to provide a number of rights to persons investigated for criminal offenses and to those convicted.

With the first group, the right to a fair trial is recognized, a number of directives being adopted over time on the right to interpretation and translation (2010), the right to information in criminal proceedings (2012), the right to be assisted by a lawyer in criminal proceedings and the right to communicate after arrest (2013).

With respect to detainees, a resolution was adopted in 2011 which called for the establishment of common standards regarding detention conditions.

The tools listed above mainly come to support investigators, providing them with different levers that streamline the fight against crime. Legislation elements are also introduced to protect persons under investigation or convicted from any abuses.

2. EUROPOL

EUROPOL was created in the European Union to ensure a safer common area and to combat serious crime effectively. It has been operational since 1999, due to increased risks posed by terrorism and serious organized crime.

EUROPOL is the European Union agency for the enforcement of law and carries out support activities against criminal activities with the highest risk for the security of the Union, such as

- terrorism;
- international drug trafficking;
- money laundering;
- trafficking in human beings;
- cybercrime;
- counterfeiting of the euro currency;
- illegal migration.

The Agency also assists in the investigation of crimes such as:

- intellectual property crimes;
- cigarette smuggling;
- tax evasion.

In order to achieve its objectives, EUROPOL works with law enforcement institutions in the 28 EU Member States and in non-EU states such as Australia, Canada, the USA and Norway.

2.1. Exchange of information

The main activity of Europol is to obtain, analyze and disseminate information on organized crime networks and terrorism. Moreover, the agency does not have the right to

[4]http://www.europarl.europa.eu/aboutparliament/ro/displayFtu.html?ftuId=FTU_5.12.6.html.

make direct arrests but it can coordinate actions to combat criminal groups. Thus, the agency participates annually in about 18,000 investigations[5].

For the exchange of information, the agency has an efficient and secure infrastructure. In this respect, it benefits from modern instruments such as SIENA[6] which allows for a confidential exchange of data between the States concerned, providing a high capacity for interoperability with other systems at European level and other cooperating states. For example, SIENA allowed in 2012 the initiation of 15,949 cases and 414,334 operational messages were exchanged.

EUROPOL also incorporates EIS[7], which comprises data on the individuals involved and other related data to support Member States, Europol and its cooperation partners in their fight against organised crime, terrorism, and other forms of serious crime[8].

In order to strengthen its position as a platform for specialty areas and to facilitate knowledge and communication exchange between different communities of experts, Europol developed the Europol Platform for Experts (EPE)[9]. Within EPE there are currently 25 online communities on various topics, such as:

- combating terrorism;
- European anti-corruption training;
- intellectual property crimes, etc.

In addition to these tools in the fight against serious crime cases, EUROPOL also provides data analysis. Thus, Member States benefit from operational analysis providing data management and centralization, as well as strategic analysis. The latter is a genuine tool that supports decision makers in the fight against organized crime. They can make the most appropriate decisions to stop the scourge.

2.2 JIT

The instrument with the best results in the fight against serious crime is JIT (joint investigation team). It consists of a joint investigation team constructed under an agreement between two or more EU countries for a fixed period to investigate a particular case. JIT can also involve non-EU states, with the approval of the other states involved.

JIT offers several benefits, such as:

- information is shared directly between JIT members without the need for formal requests;
- Letters Rogatory are dispensed while the investigative measures can be requested between team members directly. This also applies to requests for coercive measures;
- JTI members may participate in house searches, interrogations and other specific measures. This measure helps to overcome language barriers;
- ability to coordinate efforts on the spot and for informal exchange of specialised knowledge;
- ability to build and promote mutual trust between practitioners from different jurisdictions and work environments;
- a JIT provides the best platform to determine the optimal investigation and prosecution strategies;
- ability for Europol and Eurojust to be involved by direct support and assistance.[10]

[5]https://www.europol.europa.eu/content/page/about-us.
[6] N.A. - Secure Information Exchange Network Application.
[7] N.A. - Europol Information System.
[8]https://www.europol.europa.eu/content/page/europol-information-system-eis-1850.
[9]https://www.europol.europa.eu/content/page/europol-platform-experts-1851.
[10]https://www.europol.europa.eu/sites/default/files/st15790-re01.ro11.pdf.

JIT is usually organized when investigating serious forms of crime, where research is difficult and requires the involvement of other Member States.

2.3. European Cybercrime Centre (EC3)

Within EUROPOL, as a measure against the existing challenges to European security, EC3 was created. This occurred due to the fact that the Internet and information systems play an important role in our daily activities. More and more personal or commercial data is exchanged by using them. Thus, computer fraud or attacks are increasingly common, estimating that, worldwide, victims suffer annual losses of about 290 billion Euros[11].

It is a centre for cybercrime and addresses the following deeds:

- online frauds committed by organized groups to obtain large profits which cause serious damage to the victims;
- Infrastructure and critical information systems in the European Union.[12]

EC3, although founded in 2013, has already begun to show results. Thus, from the participation with EUROJUST and other six countries, a network that dealt with child pornography was destructured. 10 people were arrested following the action. Additionally, 30 TB[13] of data and hundreds of DVDs were seized.

3. EUROJUST

It was established in 2002 to support and strengthen coordination and cooperation between the Member States of the European Union in an effort to combat crimes in the range of serious crime in all phases of criminal prosecution. Eurojust also has in its jurisdiction the solving of problems that arise in the investigation process due to varying legislation of the Member States.

Eurojust is composed of one representative for each of the 28 Member States, called a national member. This member could be from among prosecutors, judges or police officers.

Eurojust has a number of key roles and powers, which are granted to it under the Eurojust Decision. For example, it responds to requests for assistance from competent national authorities of the Member States. In return, Eurojust can ask the Member States to undertake criminal investigations or prosecutions of specific deeds.

Eurojust also helps to resolve conflicts of jurisdiction where more than one state is in a position to undertake an investigation or prosecution in a particular case. Eurojust facilitates the execution of international judicial instruments such as the European Arrest Warrant. It also provides funding for the setting up and operational needs of Joint Investigation Teams.[14]

Eurojust focuses its efforts on the following deeds:

- trafficking in persons;
- illegal migration;
- cybercrime;
- reducing the production and distribution of synthetic drugs;
- trafficking in illicit goods.

[11]https://www.europol.europa.eu/ec/cybercrime-growing.
[12]https://www.europol.europa.eu/ec3.
[13]https://www.europol.europa.eu/latest_news/international-network-child-abuse-photographers-dismantled.
[14]http://www.eurojust.europa.eu/Pages/languages/ro.aspx.

Conclusions

At EU level, activities are conducted continuously to combat serious crime.

In addition, efforts are constantly made to identify the best solutions to fight against serious crime, find new solutions and improve existing ones.

In the field of judicial cooperation at criminal level, numerous improvements were noted. From the emergence of the European extradition mandate to the creation of bodies such as Europol and Eurojust.

Another beneficial element is the creation of JITs. They substantially improve joint activities, making them more efficient and eliminating bureaucratic issues or legislative differences.

The efficiency of tools and institutions fighting against serious crime is proven by numerous activities, the results of which are positive. Thus nowadays about 1,400 cases are investigated annually within Eurojust.

BIBLIOGRAPHY:

1. http://europa.eu/legislation_summaries/justice_freedom_security/judicial_cooperation_in_criminal_matters/index_ro.htm.
2. http://www.eurojust.europa.eu/doclibrary/corporate/eurojust%20Annual%20Reports/Annual%20Report%202013/Annual-Report-2013-RO.pdf.
3. http://www.eurojust.europa.eu/Pages/languages/ro.aspx.
4. http://www.europarl.europa.eu/aboutparliament/ro/displayFtu.html?ftuId=FTU_5.12.6.html.
5. https://www.europol.europa.eu/content/page/about-us.
6. https://www.europol.europa.eu/content/page/europol-information-system-eis-1850.
7. https://www.europol.europa.eu/content/page/europol-platform-experts-1851.
8. https://www.europol.europa.eu/ec/cybercrime-growing.
9. https://www.europol.europa.eu/ec3.
10. https://www.europol.europa.eu/latest_news/international-network-child-abuse-photographers-dismantled.
11. https://www.europol.europa.eu/sites/default/files/st15790-re01.ro11.pdf.
12. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/248645/Serious_and_Organised_Crime_Strategy.pdf.

BIOLOGICAL WAR – UNCONVENTIONAL COMPONENT OF THE HYBRID WAR

Florian RĂPAN
Major General (Ret.), PhD Professor within "Dimitrie Cantemir" Christian University, Bucharest, Romania.
E-mail address: rapan_florian@yahoo.com

Dana-Silvia CONTINEANU
Legal expert within ANT, PhD student in Sociology, Research Institute for Quality of Life – Romanian Academy, PhD candidate in Military Sciences, "Carol I" National Defence University, Bucharest, Romania.
E-mail address: dscconti@yahoo.com

Abstract: *The war presented today, in a global world, faces that were unthinkable at least 30 years ago. The combat forces are not conventional war against terrorism being either one (which takes a global and unconventional form) or one regional and worn between the armed forces and the so-called civilian forces or one with cyber origin which was worn on a virtual plan. This raises the notion of hybrid war, and in this paper we want to identify the components of this type of war, but also to point out the importance of the biological component of this kind of war.*

Key words: *terrorism, biological war, hybrid war, armed forces, civilian forces.*

1. The hybrid war – the biological war

What is war? The war is an armed conflict, lasting, between two or more nations, states, human groups, in order to achieve economic and political interests.

The history of humanity has known and experienced many types of war such as civil war, cold war, psychological war, total war and nowadays has faced the war against terrorism. Following the conflict from Ukraine, the hybrid war was included more often in the classification of the types of war.

Vladimir Gerasimov, Chief of Staff of the Russian Armed Forces, wrote in an article in February 2013, that war and peace are concepts whose boundaries are increasingly blurred. He argues that "the methods of conflict" are changed, which contains "the massive recourse to political, economic, informational, humanitarian and other non-military measures". Also he quoted the Soviet military theorist Georgii Isserson: the mobilization does not intervene when war is declared, but "unnoticed, occurs long before that"[1].

In 2004, NATO was conducting theoretical research with the participation of thousands of experts who have had the conclusion that future wars will be mostly hybrid wars[2].

The hybrid war involves both armed forces and paramilitary forces which are using conventional and unconventional means of fighting. If we analyze these combinations of

[1] *Ce este războiul hibrid dus de Rusia în Ucraina şi cum a fost el pregătit de zece ani sub ochii permisivi ai Occidentului*, 1 septembrie 2014, http://www.hotnews.ro/stiri-international-18014446-este-razboiul-hibrid-dus-rusia-ucraina-cum-fost-pregatit-zece-ani-sub-ochii-permisivi-occidentului.htm.

[2] Armand Gosu, *Ucraina, un altfel de război*, în „Revista 22", 29 aprilie 2014, http://www.revista22.ro/ucraina-un-alt-fel-de-razboi-40962.html.

forces and means which are taking part in such wars, we can say that the fight against terrorism is a hybrid war, but the terrorist act itself can be considered an act of hybrid war. We support it because in both types of combat the casualties can be civilian, military or militarized casualties and in both cases is to achieve political and/or economic interests, and the means of mobilizing are unnoticed before the start of the trigger itself. The steps of hybrid war can be materialized through cyber-attacks, economic activities which create vulnerabilities to the enemy, attacks allegedly terrorist attacks, infiltration in the target state society through cultural and, why not, by using biological weapons. In last case, appears the notion of biological war as a component and a possible way of manifestation of the hybrid war.

In the international law, the biological weapons are expressly prohibited; they are weapons of mass destruction, with effects that cannot be limited in time and space that cannot be predicted with certainty as effects. This means that they can have a destructive effect on a long period of time and on a big perimeter. These effects cannot be predicted or estimated precisely.

The biological weapons can contain biological agents such as bacteria, viruses, and pathogenic fungi, bacterial or fungal toxins. We must mention that these biological agents are those which are naturally occurring in the environment, but it can be engineered pathogens to develop and obtain new ones with qualities which cannot be naturally occurring in the environment and can cause more powerful adverse effects on the target. Please note that a biological weapon is not required to produce a lethal effect, it is sufficient to have an incapacitating effect for limited periods of time, sometimes with squeals.

By comparison to other weapons of mass destruction, the biological weapons require low cost of production and processes are relatively easy, sometimes being able to obtain a delay of the biological effect of such weapons. Also specific to this type of weapons are multiple possibilities dispersing latency response to pathogen infection (hides easily be biological attack by its appearance as an usual epidemic situation), the extensive morbidity damage to living organisms, the difficulty of detecting biological agents and the difficulty of achieving protection against the biological weapon.

For a better understanding of the devastating effects of this component of a possible hybrid war, we must know what involves the preparing of a biological warfare, namely:

- It is an activity which begins to be realizes since peacetime;
- It includes basic research for the selection of biological agents that have suitable properties to the proposed goals;
- The production of selected biological agents in sufficient quantities to achieve the desired results from their use;
- The storage of biological agents in optimal conditions to preserve intact their destructive qualities;
- The implementation and preparing the necessary means for the dispersion of biological agents;
- Testing the biological attack, either real or in a simulated way[3].

We underline that the biological weapon can be used both strategically and tactically-operative. Thus, from a strategic perspective it can be used to disrupt the defense system and supply, and from the tactically-operative perspective it can be used both offense and defense, including in human and animal agglomerations.

[3] Viorel Ordeanu, Adrian A. Andrieş, Lucian Hîncu, *Microbiologie şi protecţie medicală contra armelor biologice*, Editura Universitară „Carol Davila", Bucureşti, 2008, p. 11.

2. The health strategy considerations in biological warfare

A concern about significant damage to the enemy existed worldwide from the earliest times, an example being the case of the Russo-Swedish war in 1719, when Russian troops besieging the city of Reval caused a plague among Swedish troops through contaminated human cadavers disposal over the city walls.

During the First World War were epidemics, but could not definitely prove the use of biological weapons. However, there were concerns and efforts on banning the use of biological weapons but also interest in research and development.

Thus, in the 30s the Japanese and Russians conducted research on the use of biological weapons and Germany conducted secret tests of such weapons during the Second World War.

To better understand the devastating impact of a biological attack is enough to remember the production plant bombs containing biological agents to combat, plant which was commissioned in 1943 at Camp Detrick in Scotland. It should be noted that the soil of the island remained contaminated with anthrax for many years, and in 1979 it was ordered to decontaminate the soil by using 283 tons of formaldehyde, the island being declared decontaminated until 1988[4].

Despite of all the research in the development of biological weapons, in the Second World War such weapons were not used. The research and development of biological weapons continued after the Second World War, USA and Russia being interested in this field.

The humanity has realized the danger of this type of weapon and on 10 April 1972 opened for signature *Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction* at London, Moscow and Washington. The Convention entered into force on 26 March 1975. It was adopted by UN General Assembly Resolution no. 2826 (XXVI) and is complementary to "Protocol prohibiting the use in war of asphyxiating gases, toxic or similar means of fighting bacterial", protocol which was signed on 17 June 1925 in Geneva.

A total of 154 states have signed the convention, but there are countries that have not signed it and continued research and development of biological weapons. Romania ratified the Convention by Decree no. 253/1979 ratified on 25 July 1979. The text of the Convention provides that states - parties can not acquire or hold biological weapons in any circumstance[5]. The convention also prohibits signatory states the development, production, stockpiling or acquisition of biological or toxic agents if there is justification for their use for peaceful purposes.

Among the agents that can be used as weapons are aflatoxin, mycotoxins, drug resistant tuberculosis, typhus and others that may contaminate food, water and man causing diseases that can lead to death. Biological weapons can be easily spread in the air, water and land so as to be easily inhaled and consumed by humans. Usually, they have as effect the death in a few weeks or months. The biological attack (terrorist or otherwise) cannot be quickly identified because symptoms usually resemble normal conditions or manifestations thereof.

It should be noted that in the EU there is an *early warning system* of notification of serious incidents and severe adverse effects for the Member States to prevent outbreaks and hence biological attacks. USA has created a detection system that generates a preliminary warning that deadly germs are released into the atmosphere[6].

---

[4] Stan Petrescu, *Ameninţări Primare*, Editura Militară, Bucureşti, 2008.
[5] *Neproliferarea armelor biologice*, www.mae.ro.
[6] Stan Petrescu, *op. cit.*, 2008, p. 214.

Beyond the issues mentioned above, Romania, as a NATO and EU Member State, should consider the possibility that participating as an actor in a hybrid war, can be a victim or forward (in the NATO forces). This requires some tactical health considerations, in spite of the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, especially since there is information that some countries have fully working laboratories and plants specialized in the research and production of biological weapons. There are states that allocate funds for research programs that aim to solve problems on applications in biological warfare. There is also some information that terrorist organizations intend to use biological weapons in a possible terrorist attack. An example of this is the case of ISIS's plans for a biological attack with bubonic plague.

During a raid on a hideout ISIS Syrian province of Idlib, near the border with Turkey, it was discovered a laptop of an ISIS member. The laptop contained thousands of data files and secret plans, including the ones for the bubonic plague biological attack. The data found indicated that the advantage of a biological weapons attack is that does not cost much, while casualties are enormous. The information stored on the laptop contained data on how the chemical weapons factory can be prepared for a potential attack, with catastrophic global consequences. Information on biological attack was written in Arabic, in its 19 pages, noting how can be tested the biological weapon used in the attack.[7]

The ISIS case shows the determination of terrorists to achieve their purpose, and that it is possible such an attack anytime during the hybrid origin terrorist war which they bear to the civilized world.

Another possibility of biological attack is narrated by captain Al Shimkus, Professor of National Security Affairs at the Naval War College in the United States, that the group Islamic State or any other terrorist organization could use Ebola virus as a biological weapon. The way how they would perform biological attack plan would materialize through the use of infected people, so the virus can be spread through the international aviation system. "The individual would be exposed to Ebola virus would be the carrier", said the captain Al Shimkus Forbes. He added that "In the context of terrorist activity is not too sophisticated to reach the next step, to use people as carriers" of the virus. Also, captain Shimkus also said that the group Islamic State could send intentionally some of its members to areas affected by the epidemic of Ebola, to Ebola virus spike and then they can contaminate as many people in the countries covered by their attack.[8] We may say that it appears a new type of kamikaze namely biological, so we will have a biological terrorist kamikaze.

It should also be noted that the effect of biological weapons may be enhanced by combining them with nuclear, chemical and incendiary, having as result serious injuries which are treated with difficulty. The biological attacks can be massive, dispersed and diverse, affecting tactical objectives, operational and/or strategic objectives behind the front or in a unitary to obtain a rapid military decision.

Also, we must remember the fact that in case of a hybrid war we can have a cyber attack on the electronic and IT infrastructure for commanding and controlling the national system of emergency medical services, biological attack on the armed forces and the civilian population and the environment ... and the possibility of counteraction is ... 0. It's just a grim scenario, but that should not be ignored and it draws the attention to the danger of hybrid war.

---

[7] Harald Doornbos, Jenan Moussa, *Found: The Islamic State's Terror Laptop of Doom*, in "Foreign Policy", 28 August 2014, http://www.foreignpolicy.com/articles/2014/08/28/found_the_islamic_state_terror_laptop_of_doom_bubonic_plague _weapons_of_mass_destruction_exclusive.

[8] Ioana Bojan, *Gruparea Stat Islamic ar putea folosi Ebola ca armă biologică, avertizează un expert american*, 5 octombrie 2014, http://www.mediafax.ro/externe/gruparea-stat-islamic-ar-putea-folosi-ebola-ca-arma-biologica-avertizeaza-un-expert-american-13365566.

3. The response of the international community – countermeasures

The international community, for the most part, is firm in its rejection of the threat or possible biological attacks, and this has resulted in the last NATO Summit. The its Declaration, NATO urged all Member "to commit to combating effectively the proliferation of WMD through the universalisation of the Chemical Weapons Convention, the Biological and Toxin Weapons Convention, the Comprehensive Nuclear Test Ban Treaty and through the Proliferation Security Initiative"[9]. Also, NATO states have reiterated that they are "postured to counter Chemical, Biological, Radiological, and Nuclear (CBRN) threats, including through the Combined Joint CBRN Defence Task Force"[10].

As concerning to counter biological attacks, NATO Member States will consider that their information is correct and up to date so that the capacities involved in prevention, protection and counter this type of attack to be appropriate and effective. Also, based on the *Defence against Terrorism Programme of Work* the capabilities and technologies of NATO states will be enhanced and developed to provide protection against CBRN threats.

At the United Nations, was unanimously adopted The Security Council Resolution 1540 (2004)[11], which established a program of action and prevents the proliferation of nuclear, chemical and biological weapons. The Security Council has decided that all States shall refrain from providing any form of support to non-State actors that attempt to develop, acquire, manufacture, possess, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery. The resolution requires to all States to adopt and enforce laws to get that effect. It also requires them to develop and maintain border controls and law-enforcement efforts to detect, deter, prevent and combat, including through international cooperation when necessary, the illicit trafficking and brokering in such items in accordance with their national legislation, and consistent with international law.

In May 2014, at one decade after the adoption of the Resolution, UN Member State are working hard on The Security Council committee established pursuant to the resolution (1540 Committee) is required to report on implementation of the text's provisions. Security Council resolution 1977 (2011) extended the Committee's mandate until 25 April 2021[12].

On October 2014, the U.S. Government has taken steps to promote and enhance the USA's biosafety and biosecurity, including immediate and longer term measures to review activities specifically related to the storage and handling of infectious agents. According to The White House's Office of Science and Technology Policy press release, "the U.S. Government will institute a pause on funding for any new studies that include certain gain-of-function experiments involving influenza, SARS, and MERS viruses. Specifically, the funding pause will apply to gain-of-function research projects that may be reasonably anticipated to confer attributes to influenza, MERS, or SARS viruses such that the virus would have enhanced pathogenicity and/or transmissibility in mammals via the respiratory route"[13].

---

[9] *Wales Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales*, Press Release (2014) 120, 5 September 2014, http://www.nato.int/cps/en/natohq/official_ texts_112964.htm.

[10] Ibidem.

[11] United Nations, *Security Council Resolution 1540 (2004): Non-proliferation of weapons of mass destruction*, 28 April 2004, http://daccess-ods.un.org/TMP/2814533.41245651.html.

[12] *Ten Years after Adoption of Security Council Resolution 1540 (2004), Member States Working Hard to Implement Its Requirements*, UN Press Release, 6 May 2014, http://www.un.org/press/en/2014/dc3496.doc.htm.

[13] *Doing diligence assess risks and benefits life sciences gain function research,* White House's OSTP Press Release, 17 October 2014, http://www.whitehouse.gov/blog/2014/10/17/doing-diligence-assess-risks-and-benefits-life-sciences-gain-function-research.

Conclusions

The biological war is an element of the hybrid warfare. It is carried by unpredictable rules in terms of the type of biological agents, the type and location of the attack. The only common element is the use of biological agents, but the target may consist of any living element. The effect of such an attack can not be quantified as the number of victims and the consequences in the short, medium and long term. Indeed, in a hybrid war is quite unusual the use of biological war, most combatants being focused on armed attacks, economic attacks, cyber attacks or attacks with social impact, but it is not negligible the annihilation of the opponent by creating a state of helplessness and difficulty in his reactions, of physical pain and ultimately death, in a way that no one could detect the real source of these effects.

In the framework of these conclusions, we think it is necessary to recall aspects of the NATO Summit in Wales, which although not specifically nominate bio-threats but it is yet contained as notion. In paragraph 1 of the Preamble to the Declaration, NATO member states stated that, "Growing instability in our southern neighbourhood, from the Middle East to North Africa, as well as transnational and multi-dimensional threats, are also challenging our security". NATO Member State reiterates the danger of the weapons of mass destruction, including nuclear and cyber attacks[14]. In light of these statements and the quality of Romania's membership of NATO, we believe it is necessary to develop consistent policies and procedures for possible hybrid war situations.

BIBLIOGRAPHY:

1. BOJAN, Ioana, *Gruparea Stat Islamic ar putea folosi Ebola ca armă biologică, avertizează un expert american*, 5 octombrie 2014, http://www.mediafax.ro/externe/gruparea- stat-islamic-ar-putea-folosi-ebola-ca-arma-biologica-avertizeaza-un-expert-american-13365566.
2. DOORNBOS, Harald; Jenan MOUSSA, *Found: The Islamic State's Terror Laptop of Doom*, in "Foreign Policy", 28 August 2014, http://www.foreignpolicy.com/articles/2014/08/28/found_the_islamic_state_terror_laptop_of_doom_bubonic_plague_weapons_of_mass_destruction_exclusive.
3. GOSU, Armand, *Ucraina, un altfel de război*, în „Revista 22", 29 aprilie 2014, http://www.revista22.ro/ucraina-un-alt-fel-de-razboi-40962.html.
4. ORDEANU, Viorel; Adrian A. ANDRIEŞ, Lucian HÎNCU, *Microbiologie şi protecţie medicală contra armelor biologice*, Editura Universitară „Carol Davila", Bucureşti, 2008.
5. PETRESCU, Stan, *Ameninţări Primare*, Editura Militară, Bucureşti, 2008.
6. *Ce este războiul hibrid dus de Rusia în Ucraina şi cum a fost el pregătit de zece ani sub ochii permisivi ai Occidentului*, 1 septembrie 2014, http://www.hotnews.ro/stiri-international-18014446-este-razboiul-hibrid-dus-rusia-ucraina-cum-fost-pregatit-zece-ani-sub-ochii-permisivi-occidentului.htm.
7. *Doing diligence assess risks and benefits life sciences gain function research,* White House's OSTP Press Release, 17 October 2014, http://www.whitehouse.gov/blog/2014/10/17/doing-diligence-assess-risks-and-benefits-life-sciences-gain-function-research.
8. *Neproliferarea armelor biologice*, www.mae.ro.

[14] *Wales Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales*, Press Release (2014) 120, 5 September 2014, http://www.nato.int/cps/en/natohq/official_ texts_112964.htm.

9. *Ten Years after Adoption of Security Council Resolution 1540 (2004), Member States Working Hard to Implement Its Requirements*, UN Press Release, 6 May 2014, http://www.un.org/press/en/2014/dc3496.doc.htm.
10. United Nations, *Security Council Resolution 1540 (2004): Non-proliferation of weapons of mass destruction*, 28 April 2004, http://daccess-ods.un.org/TMP/2814533.41245651.html.
11. *Wales Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales*, Press Release (2014) 120, 5 September 2014, http://www.nato.int/cps/en/natohq/ official_ texts_112964.htm.

"SOFT POWER" INSIDE THE PROCESSESOF CONFLICT PREVENTION AND CRISIS MANAGEMENT

Sînziana-Florina IANCU
PhD candidate, Lieutenent with the research domain: "Information and National Security",
"Carol I" National Defence University, Bucharest, Romania.
E-mail address: iancu_sanziana@yahoo.com

***Abstract**: The need for national and international crisis management has brought to the fore many strategies developed by different methods of analysis and research. Over time, the concept of "soft power" was revealed and has become an indispensable element in international cooperation and very close related to public diplomacy. With the development of the media, of informatics and technological developments, the role of "soft power" has increased, becoming the essential element in diplomacy. Even though the purpose of "soft power" is basically positive, the line between it and the actions of propaganda and aggression through information can be easily violated. This can only lead to results that are even more offensive than "hard power" by using psychological measures designed for the benefit of only one party at the expense of the other / others. It is therefore important that before using this tool, the deciders should define their goals and expectations.*

***Keywords:** "soft power", diplomacy, information, "hard power", crisis, cooperation, management.*

Introduction

The concept of "soft power" became known around the '90s through Joseph Nye, proposing alternative approaches of the concept of "conflict" at the expense of means of force and aggression. This kind of actions involved non-invasive methods, by the usage of cultural diplomacy, persuasion and negotiation, tools that were considered as being more beneficial than the use of force and military counter-offensive or offensive elements. Such an example is the development of strong PR techniques, through media for influencing the public opinion, which can have a much faster, inexpensive and beneficial impact. "Soft power" could be regarded as a component of diplomacy that makes use of all the effects of globalization, applying significant psychological methods. An implementation of this concept to the detriment of the concept of "hard power" has begun having a decisive success, by taking into account the economic factor. Thus, it was concluded that using techniques of "soft power" implies, from a financial point of view, less resources than those necessary for an armed conflict.

Inside the "soft power" method, there are state's cultural strengths that can be found, by promoting traditions and customs of the state. Thus, through cultural force, public opinion may be more easily influenced, and decision makers could become quickly controlled. The way that a state's historical heritage is being presented and valued may form strong communication links, but at the same time, may deepen pre-existing conflictual rifts.

1. "Soft Power" as a cultural diplomacy basic instrument

The existence of cultural diplomacy determines new shapes and meanings for the global competition. In this way, the economic strength and military power get to be subsidiary

to "soft power". In order to maximize the mechanisms of "soft power", further development and adaptation of the intelligence domain are needed.

This concept is actually based on two main pillars (see Figure no. 1):

1. ways to attract, not coercion;
2. intrinsic values that are less tangible.

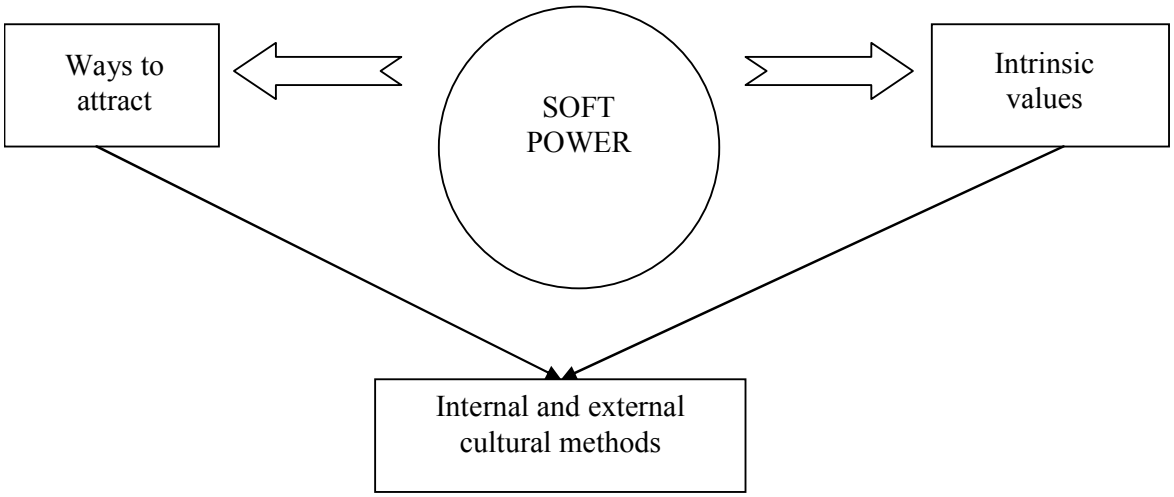


Figure no. 1. "Soft power" components

A State may establish and strengthen its means of "soft power" through actions that involve the popularization of its own image, using external and internal cultural means. External cultural resources consist of the organization of conferences, internships, scholarships for foreign students, offering jobs to foreign citizens, cooperation in international projects, festivals and sporting events, producing films and programs.

Internal resources are based on encouraging cultural and educational policies and on providing financial support to those institutions that promote the image of the state, by drawing attention to stakeholders, by attracting collaboration and ultimately, by attracting people that are able to develop and to bring added value to the organization and the state (the last and the most important beneficiary).

Currently, the Euro-Atlantic culture dominates the whole world, so globalization has a very important role. The main promoter of "soft power", on the regional scale, having global influences, may be seen as EU, that does not have military interests or capabilities, and that is mainly represented in areas of economics, society and politics. According to some analysts, like Michael Clarke, the EU capability to support a peaceful approach is limited on a long perspective, and that is because its strategy to promote economic interdependence, international institutionalism and the perspective of accession to a thriving economic community is difficult to achieve in the context of unexpected frequent crises.[1] Going even further, some authors believe that the very ideas promoted by the EU are the crisis culprits.

[1] Lucian JORA, *Securitatea de tip soft*, „Enciclopedia relaţiilor internaţionale", p. 99 apud M., Clarke, *Future Security Threats and Challenges*, Pappas S.A., S.Vanhoonacker (eds) *The European Union's Common Foreign and Security Policy: The Challenges of the Future, Maastricht*, European Institute of Public Administration, 1996, http://revista.ispri.ro/wp-content/uploads/2012/09/97-104-Enciclopedia-Relatiilor-Internationale.pdf, accesat la data de 19.06.2014.

Christopher Hill believes that the EU's advantage over other players is that its long-term efforts are aimed at changing the environment itself that is the origin of these crises.[2]

Cultural diplomacy is the reference of "soft power", which is accessible to a large mass of people, having as a primary objective – informing people. This does not imply political or economic ramifications, at least not visible ones, and it doesn't have a combative structure, but rather peaceful. Cultural diplomacy has a variety of information sources, being different to propaganda actions that come from a single controlled and precisely targeted source.[3] Furthermore, this kind of diplomacy suggests the existence of dialogue, malleability in negotiation processes and adaptability to the change. In this regard, by the resolution adopted by the EU Parliament on 12 May 2011, the EU is guided to highlight as many cultural aspects in its diplomatic efforts to promote human rights, the democratic issues and support the development of the member states.

Thus, the resolution "stresses the need for all EU institutions to recognize more fully the value of culture as a force for tolerance and understanding and as a tool for growth and more inclusive societies, [also] stresses that democratic and fundamental freedoms, such as freedom of expression, press freedom, freedom from want, freedom from fear, freedom from intolerance, hatred and the freedom to access printed and digital information, as well as the privilege to connect and communicate – online and offline – are important preconditions for cultural expression, cultural exchanges and cultural diversity, [it] recalls the importance of the cultural cooperation protocols and their added value in bilateral agreements on development and trade [and] emphasizes that transatlantic cooperation and cooperation with neighboring European states is important to advance joint interests and common values"[4].

Through its programs, UE "states that cultural and educational exchanges can potentially strengthen civil society, foster democratization and good governance, encourage the development of skills, promote human rights and fundamental freedoms and provide building blocks for lasting cooperation"[5].

In matters of diplomacy and cultural cooperation, the EU resolution "emphasizes the importance of cultural diplomacy and cultural cooperation in advancing and communicating throughout the world the EU's and the Member States' interests and the values that make up European culture; stresses the need for the EU to act as a (world) player with a global perspective and global responsibility; argues that the EU's external actions should focus primarily on promoting peace and reconciliation, human rights, international trade and economic development, without neglecting the cultural aspects of diplomacy; stresses the need to devise effective strategies for intercultural negotiations, and considers that a multicultural approach to this task may facilitate the conclusion of beneficial agreements, putting the EU and third-country partners on an equal footing; emphasizes the need to adopt a comprehensive approach to cultural mediation and cultural exchange and the role of culture in fostering democratization, human rights, conflict prevention and peace-building; encourages the launch of policy dialogues on culture [… and] encourages the setting of priorities directly linked to the cultural dimension within the EIDHR, including strengthening the rule of law,

[2] Idem apud Cristopher, Hill, *The Actors in Europe's Foreign Policy*, London, Routledge, 1996, articol preluat de pe site-ul http://revista.ispri.ro/wp-content/uploads/2012/09/97-104-Enciclopedia-Relatiilor-Internationale.pdf, accesat la data de 19.06.2014.

[3] Lucian, Jora, *Diplomaţia culturală*, „Enciclopedia relaţiilor internaţionale", p. 101, articol preluat de pe site-ul http://revista.ispri.ro/wp-content/uploads/2012/09/97-104-Enciclopedia-Relatiilor-Internationale.pdf, accesat la data de 19.06.2014.

[4] European Parliament resolution of 12 May 2011 on the cultural dimensions of the EU's external actions (2010/2161(INI)), http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2011-0239&language=EN , accesat la data de 19.06.2014.

[5] Idem.

conflict management and prevention, civil society cooperation and the role of new technologies as regards freedom of expression, democratic participation and human rights."[6]

The "soft power" method touches various areas of life, being used to pursue different group interests and involves accessible resources without harming or destroying. "soft power" approach can be introduced in areas such as economics (business and technology) in education and training, foreign policy, etc. (Figure no. 2).

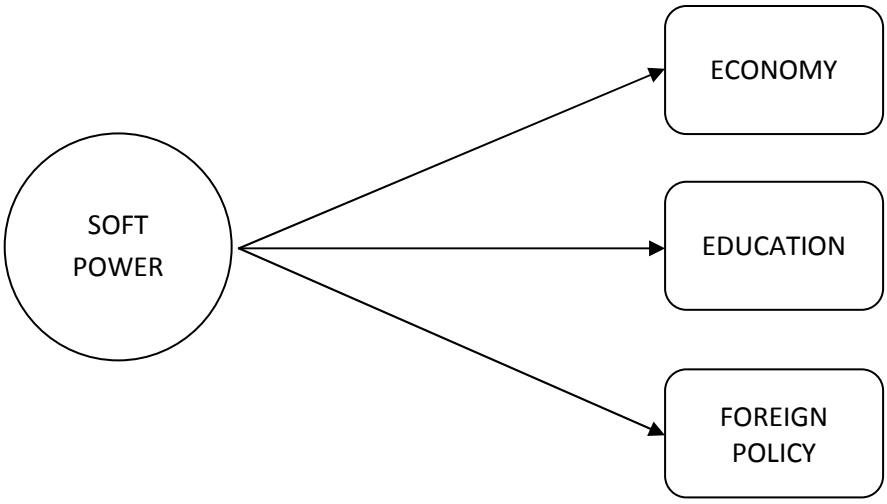


Figure no. 2. Possible domains where „soft power" may be applied to

In fact, "soft power" is a social stake using psychological techniques (persuasion, manipulation, negotiation), inside a favorable geopolitical context or as a result of (potentially) bad socio-political conditions. In unfavorable conditions, such as a crisis, "soft power" manifests through diplomatic cooperation techniques and attempts of persuasion of the opponents, though in the context of normal conditions of a State, "soft power" appears as an instrument of globalization and influence of other global players in its favor. "Soft power" is the art of persuading others (even the enemies) to act on your behalf, without forcing them.

Unlike the "hard power", this component of public diplomacy has numerous benefits: low cost, controlled risk management, non-existing human losses, even economic gains. In the context of a state gaining popularity through strategies of attracting others, it has become quite clear that more and more individuals (foreigners) will travel or develop different business, thus investing in the economy of that state. "Soft power" is characterized by elements such as transformational leadership, flexibility in the negotiation process, adaptability to possible changes of the context (see Table 1).

	SOFT POWER	HARD POWER
ADVANTAGES (SOFT POWER) VERSUS DESADVANTAGES (HARD POWER)	Low costs	High budgetary resources (in case of a conflict: military maintenance, investment and advanced technology implementation, maintenance of weapons, etc.)
	Controlled risk management	Possible unexpected and undetectable risks
	Inexistent human losses	Unavoidable human and

[6] *Idem*.

		material losses
	Economic gain	Economic losses (especially in case of defeat)
FEATURES	Transformational leadership	Transactional leadership
	Flexibility inside the negotiation process	Rigidity in the negotiation process (categorical terms, ultimatums)
	Adaptability to possible environmental changes	Difficulty in what concerns a potential tactical modification
	Values the INDIVIDUAL	Values the STATE
	"Soft power" instruments are not always under government's control	The government controls and applies "hard power" methods
	Benefits and results appear after a long period	Results appear, usually, in a shorter period
	The advantage of "soft power" can easily disappear in case of losing credibility	"Hard power" can evolve in the absence of credibility (especially in this case)

Table no. 1. "Soft power" versus "hard power"

"Soft power" can be considered as part of public and cultural diplomacy, with common elements and serving the interests whose outcome can be achieved through such diplomatic strategies. Public diplomacy is represented by the transparency to other societies, specifically in communicating the national objectives and values to other actors through numerous techniques of information, such as television and/or Internet, by creating and producing shows with a global / regional nature on international topics, educational exchanges, publications aimed at a wide audience that would cross beyond borders etc. Also, public diplomacy means understanding the culture, history, psychology and language of other nations, in order to improve and develop an own culture and organization.[7] Cultural diplomacy is part of public diplomacy and helps on the improvement of cooperation between regional and global actors.

2. "Soft Power" and Information

According to Joseph Nye, "soft power" depends heavily on the credibility of state and when governments are perceived as manipulative and information is perceived as propaganda, credibility is destroyed.[8] He also considers that in a time when global information is a reality and the world is represented by a diffusion of power to non-state actors, "soft power" will become an increasingly important element in the intelligence strategies.[9] Also, to be credible in a century in which the power travels from state to non-state actors in their efforts to design [..." soft power"] governments will have to accept that power is less hierarchical information age and social. Moreover, in order to become successful in a century when power is projected from State to non-state actors, governments are being forced to accept the fact that, in an era

[7] Sergiu, Căpîlnean, *Diplomaţia Publică: Definiţie, Schimbare, Elemente*, Academia de Studii Economice, Master Geopolitică şi Relaţii Economice Internaţionale, Bucureşti, 2012, p. 2, material preluat de pe site-ul https://www.academia.edu/3201446/Diplomatia_Publica_-_Elemente_si_Definitie, accesat la data de 20.06.2014.
[8] Joseph S., Nye, *Viitorul Puterii*, Editura Polirom, 2012, Iaşi, p. 102.
[9] *Ibidem*, p. 103.

of information, power has become less hierarchical and social networks have become much more significant.

To be successful in an interconnected world means having leaders that think in terms of cooptation and not imposing.[10]

"Soft power" is based very much on information. How it is perceived leads to a context for development of methods and practices of this kind of power. Currently, the competition between states based on the information level, because information is power. However, many states posses this power, due to the huge amount of information and easy access to it. The result is an explosion of information, and this has generated a "paradox of abundance"[11]. Information abundance leads to lower attention.[12]. In these conditions, the more one is focusing on many directions, losing track of the main important information, the more powerful become those that identify the specific relevant information.

In this context, "soft power" is partly an expression of international flows of information, whose efficiency is related to them.[13] In other words, it's being created a positive image of the state, according to the intensity of these information flows, where certain political goals can be more easily achieved, and thus, many supporters may be attracted.[14] In this regard, if the image of that state / organization is more favorable, the degree of reliability is higher and State's position becomes more influential.

According to the authors[15], the informatisation domain is the most practical and effective tool in addressing "soft power", through which, a complex process of disseminating information occurs, having as immediate outcomes the increasing of message package, the maximum quality, capacity and speed receiving messages. One can thus infer that with the evolution of informational systems, the role of "soft power" in foreign policy has substantially increased. In this cycle of information inside the battle for supremacy, the largest resource of information belong to the great power States or organizations such as regional organizations with responsibility and regional or global influence.

This way, states or the large organizations that (re) confirm their position and status of power by extending influence, can be suspected of wanting to maintain and sustain the "informational-technological colonialism" which could replace the conflicts / wars, religious and financial expansions undertaken by them, so far.[16]

The application of "soft power" in international relations may be more effective in many ways, even if the results may occur later. Besides, such a choice may be helpful in preventing crises and conflict, as well as in stopping and / or reconstructing environmental stability. Even if the context of implementing "soft power" and "hard power" is the same, the conditions are different ("The tone makes the music"), and the results are more reliable and advantageous opposed to the "hard power" approach. The art of those using "soft power" is fundamentally based on the possession of information and the modality to manipulate it in a

---

[10] *Ibidem*, p. 121.

[11] Joseph S., Nye, *op. cit.*, p. 123 apud Herbert A., Simon, „Information 101: It's Not What You Know, It's How You Know It", *Journal for Quality and Participation*, July-August 1998, pp. 30-33.

[12] *Ibidem*, pp. 123-124.

[13] Valentin, Beniuc; Adriana, Beniuc, *Bazele conceptuale şi teoretice ale fenomenului „soft power"*, nr. 3-4 (7-8), 2007, Revista moldovenească de drept internaţional şi relaţii internaţionale, Institutul de Istorie, Stat şi Drept al A.Ş.M., p. 72, preluată de pe site-ul rmdiri.md/pdf/RMDIRI,%202007,%20Nr.%203-4.pdf, accesat la data de 19.06.2014.

[14] *Idem* apud Кувалдин Станислав. Бархатная перчатка для железного кулака, http://sr.fondedin.ru/new/admin/ print. php?id=1084173↑ 88&archive=108↑ 854170.

[15] *Idem.*

[16] Valentin, Beniuc; Adriana, Beniuc, *op.cit.*, p. 73 apud Багиров А.. Новые информационные технологии в международных отношениях // Международная Жизнь. № 8, 2001, p. 91.

way that would not raise reasons of doubt or that would lead to propaganda, but in a way that would seek solutions of compromise or advantage to the State practicing it.

Conclusions

In international relations, the concept of "soft power" is closely related to preventive diplomacy, using techniques of conflict prevention; however, "soft power" can also be utilized in post-conflict periods, when strategies to rebuild a stable peace environment are needed. In case of a global enemy, such as terrorism, the role of "soft power" is much stronger inside the security policies and the values which are promoted by the decision makers of the damaged states. Thus, joint mobilization efforts become a priority at the social level and mutual solidarity, through which many national and international actors try to promote their shared values, collective interests, converging lines in a spirit of cooperation and identity recognition.

One major difference between the concepts of "soft power" and "hard power" (in addition to the economic difference) is that "soft power" focuses primarily on the individual, as opposed to the vision of "hard power", where the main element is the State. Yet, paradoxically, they both have the State as the beneficiary, except that for the first one, state is the ultimate beneficiary (after the individuals), whereas for the "hard power", the first, the last and the only beneficiary, is the state. In other words, in terms of "hard power", it is essential that state interests prevail, and that its objectives are fulfilled, no matter the costs or collateral damage (including human), as often happens when conflicts / wars appear. However, in terms of "soft power", the most important value of the State is represented by the individual, therefore all its means and actions must be conducted in accordance with its interests and be used to protect and support the human being.

Acknowledgement:

This work was made possible with the financial support offered through the Development of Human Resources Sectorial Operational Program 2007 - 2013, co-financed through the European Social Fund, within the project POSDRU/159/1.5/S/138822, entitled ***"Transnational Network of Integrated Management of Intelligent Doctoral and Postdoctoral Research in the "Military Sciences", "Security and Information" and "Public Order and National Safety" Domains - a Professional Training of Elite Researchers Programme - "SmartSPODAS"."***

BIBLIOGRAPHY:

1. BENIUC, Valentin; BENIUC, Adriana, Bazele conceptuale şi teoretice ale fenomenului "soft power", nr. 3-4 (7-8), 2007, Revista moldovenească de drept internaţional şi relaţii internaţionale, Institutul de Istorie, Stat şi Drept al A.Ş.M., preluată de pe site-ul rmdiri.md/pdf/RMDIRI,%202007,%20Nr.%203-4.pdf.
2. CĂPÎLNEAN, Sergiu, Diplomaţia Publică: Definiţie, Schimbare, Elemente, Academia de Studii Economice, Master Geopolitică şi Relaţii Economice Internaţionale, Bucureşti, 2012, available at https://www.academia.edu /3201446/Diplomatia_Publica _-_Elemente_si_Definitie.
3. CLARKE, M., Future Security Threats and Challenges, Pappas S.A., S.Vanhoonacker (eds) The European Union's Common Foreign and Security Policy: The Challenges of the Future, Maastricht, European Institute of Public Administration, 1996.

4. HERBERT A., Simon, “Information 101: It’s Not What You Know, It’s How You Know It”, Journal for Quality and Participation, July-August 1998.
5. HILL, Cristopher, The Actors in Europe’s Foreign Policy, London, Routledge, 1996.
6. БАГИРОВ А.. Новые информационные технологии в международных отношениях.
7. JORA, Lucian, Diplomaţia culturală, „Enciclopedia relaţiilor internaţionale”, p. 101; articol preluat de pe site-ul http://revista.ispri.ro/wp-content/uploads/2012/09/97-104-Enciclopedia-Relatiilor-Internationale.pdf.
8. JORA, Lucian, Securitatea de tip soft, „Enciclopedia relaţiilor internaţionale” apud M., Clarke, Future Security Threats and Challenges, Pappas S.A., S.Vanhoonacker (eds) The European Union’s Common Foreign and Security Policy: The Challenges of the Future, Maastricht, European Institute of Public Administration, 1996; articol preluat de pe site-ul http://revista.ispri.ro/wp-content/uploads/2012/09/97-104-Enciclopedia-Relatiilor-Internationale.pdf.
9. JORA, Lucian, Securitatea de tip soft, „Enciclopedia relaţiilor internaţionale” apud Cristopher, Hill, The Actors in Europe’s Foreign Policy, London, Routledge, 1996; articol preluat de pe site-ul http://revista.ispri.ro/wp-content/uploads/2012/09/97-104-Enciclopedia-Relatiilor-Internationale.pdf.
10. КУВАЛДИН Станислав. Бархатная перчатка для железного кулака.
11. NYE, Joseph S.,Viitorul Puterii, Editura Polirom, 2012, Iaşi.
12. European Parliament resolution of 12 May 2011 on the cultural dimensions of the EU's external actions (2010/2161(INI)) - versiunea originală (în engleză) preluată de pe site-ul oficial http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2011-0239&language=EN.
13. ***, European Parliament resolution of 12 May 2011 on the cultural dimensions of the EU's external actions (2010/2161(INI)).

SHOULD THE WAR PRISONER'S STATUS AFTER THE 21ST CENTURY CONFLICTS BE UPDATED?

Victoria CHIRILOIU
Captain, legal branch, PhD candidate with "Carol I" National Defence University, Bucharest, Romania.

Abstract: *The war prisoner's fate is a matter of all of us. If you are a military combat personnel or just member of a military family, you must care about you or your relative future. After the Second World War, the preoccupation relating the war prisoner statute comes up with the Geneva Conventions after 12 august 1949. Despite all of the Conventions regarding military use of forces, the legality of the tools and procedures of war, the 21st century conflicts have the same problems like the ancient times. The prisoners of war are tortured; the rapes still a war weapon. Moreover, the military and conflicts science are on the evolution and the war prisoner's statute should be applied to many other persons who is involved into.*

The privatization of the security comes together with no state responsibility for the possible aggressor. The international coalition forces can also become a source of misconduct, just from the cultural diversity.

Keywords*: war, prisoners, statute, 21st century.*

Introduction

War always was a social phenomenon, no matter of time and place. If we like or not, the conflicts do not cool down with political speech or dialogs, the guns had to make noises and victims. Like any competition, one part has to loose, another wins. Time goes one, the international current and fashion changes, with the triumph of humanity principle, which says that who win must be honorable and act with generosity.

Since history, many societies were preoccupied on the way to fight and conduct the war. Avoiding the collateral victims, the inutile loss, protecting the environment, protecting the women and children, protecting the elderly, was in many cultures stated as principles into the Code of honor. In the social organizations, the right to fight was permanently opposite to the common criminal activity. If in the ancient time the code of honor into conduct was just a matter of the powerful imperators and brave commanders, the middle Ages come up with the Crusades and Cavalry principle. Since Enlightenment edges and the humanitarian principle spreading, the customary law regarding use of forces and legality of war get to the write down treaty of conventions. The milestone of the law regarding war prisoners and collateral victims is the Battle of Solferino. On 9 February 1863, in Geneva, Henry Dunant founded the "Committee of the Five" as an investigatory commission of the Geneva Society for Public Welfare. Together with the Swiss Armed Forces General Dufour, jurist Moynier, and doctors Louis Apia and Theodore Maunoir founded on 17 February 1983 the International Committee of the Red Cross[1], the most important and actual organization on the prisoner of war protection. Later the society of Red Cross had an active role into the international law issues regarding armed conflict and humanitarian actions.

The international humanitarian law is based on the most human principles, like the distinction between the enemy combatants, proportionality in the forces engaged into the

[1] The ICRC history, https://www.icrc.org/en/who-we-are/history, accessed on 16.10.2014, 12:00 hours.

conflicts, human treatments to the wounds and the one who are already captured by them enemy, military necessity and respect of the natural law, environment and cultural goods, history and international heritage.

1. Haga Conventions and Geneva Conventions stipulations

The humanitarian law was based first into the customs and regulations regarding the war on land, with focus on restriction of the weapons with the superfluous effect and inutile damages, the methods and means on warfare[2].

Into the United State territory the first Codified set of rules for war prisoner protection was the General Order 100[3], adopted by the Union Army during the Civil War[4].

On October 3, 2014, a very important representative of the ICRC in Ukraine has been killed in Donetsk. ICRC website shows up the tragedy for itself and a huge violation of the international humanitarian law, the Geneva Convention article 4. *Mr DuPasquier worked for the ICRC for more than five years carrying out assignments in Pakistan, Yemen, Haiti, Egypt and Papua New Guinea. He started his posting in Ukraine six weeks ago*[5].

Later on, after the World War II, the Red Cross organization within the whole movement for the codification of the humanitarian law, update de law regarding the victim protection during the armed conflicts. Despite the humanitarian theoreticians split doctrine of the Haga law (methods and means of warfare) and Geneva law, (victim in the armed conflict) in our opinion those branches are interdependent, the first induces the second and the second coordinates de first.

According with the Geneva Convention III regarding the POW status, only the one who respects the article 4[6] and 5 requirements can enjoy those privileges. The main requests

---

[2] History of the ICRC, the work of the ICRC is based on the Geneva Conventions of 1949, according with https://www.icrc.org/applic/ihl/ihl.nsf/vwTreatiesHistoricalByTopics.xsp, accessed on 12.10.2014, 12:00 hours

[3] Lieber Code of GO 100 all soldiers of whatever species of arms; all men who belong to the rising en masse of the hostile country; all those who are attached to the army for its efficiency, and promote directly the object of war..." as well as "citizens who accompany an army for whatever purpose, such as subtler, editors, or reporters of journals, or contractors, if captured ...."86 It was forbidden to declare that every member of a legitimate levy en masse — a spontaneous uprising of citizens in opposition to an armed invasion — would be treated as a bandit, but once the invading army had established itself as occupying force, citizens could not lawfully rise up against it.

[4] Jennifer Elsea, Treatment of "Battlefield Detainees" in the War on Terrorism, updated January 13, 2005, Legislative Attorney American Law Division, Congressional Research Service ˜ The Library of Congress.

[5]The ICRC in Ukraine, https://www.icrc.org/en/document/ukraine-icrc-delegate-killed-donetsk#.VC1IT2eSxDQ, accessed on 10.10. 2014, 12:00 hours .

[6] Prisoners of war, in the sense of the present Convention, are persons belonging to one of the following categories, who have fallen into the power of the enemy: (1) Members of the armed forces of a Party to the conflict as well as members of militias or volunteer corps forming part of such armed forces.(2) Members of other militias and members of other volunteer corps, including those of organized resistance movements, belonging to a Party to the conflict and operating in or outside their own territory, even if this territory is occupied, provided that such militias or volunteer corps, including such organized resistance movements, fulfill the following conditions: (a) that of being commanded by a person responsible for his subordinates; (b) that of having a fixed distinctive sign recognizable at a distance; (c) that of carrying arms openly; *(d) that of conducting their operations in accordance with the laws and customs of war. (3) Members of regular armed forces who profess allegiance to a government or an authority not recognized by the Detaining Power. 4) Persons who accompany the armed forces without actually being members thereof, such as civilian members of military aircraft crews, war correspondents, supply contractors, members of labor units or of services responsible for the welfare of the armed forces, provided that they have received authorization from the armed forces which they accompany, who shall provide them for that purpose with an identity card similar to the annexed model. (5) Members of crews, including masters, pilots and apprentices, of the merchant marine and the crews of civil aircraft of the Parties to the conflict, who do not benefit by more favorable treatment under any other provisions of international law. (6) Inhabitants of a non-occupied territory, who on the approach of the enemy*

of the article 4 are regarding to the honest way of fight, to show up them specific distinctions signs, respect the principle of the law of war, and follow the military type of organization. The accompany personnel of the combatants are also the beneficiary of the PoW status, also the auxiliary persons like journalist, Red Cross personnel, the aircraft crews, the contractors, if they are legally attached to the combat units. Another condition is the conduit in accordance with the international humanitarian law principle. Fighting only against the combatants, respect the principle of distinction and discrimination, military necessity, protection for the civilian population are some of the core values.

Regarding the article 4, paragraph 6, *Inhabitants of a non-occupied territory, who on the approach of the enemy spontaneously take up arms to resist the invading forces, without having had time to form themselves into regular armed units, provided they carry arms openly and respect the laws and customs of war,* what can do the civilian population during the economic and psychological war? What is the law applicable during the riots and social revolts? Are the political detainees enjoying the POW status? NO, also the one legal fighter from its side, who is called terrorist from the other side, does not enjoy the Geneva Convention III stipulation, moreover, they are punished by it, and no mentioned with the human rights benefits.

2. The Economic and Mass Media war and its victim's protections

The Public Relations schools have the main doctrine, *The arts of War*, by Sun Tzu. Media is doing real campaigns to hit their audience targets and option of persuasions. Vladimir Volkoff[7] wrote down one of the most important book regarding the invisible war launched on the media and not only, the Treaty of misinformation. Also if anyone is looking carefully and just compare into empirical way the past 20 years conflicts and war, they can figure out the scenario which is applied to most of the conflicts. The effects are showing up rapidly, the old economic institution has been damaged, the active population get out to the migration, the social depressions have been installed, there is no hope for a real, better and active life. Those are mine observational and participating remarks during the UN, Coalitions Forces and NATO missions in Angola, Former Yugoslavia and Iraq. The population behaviors were the same, just the languages other. Unfortunately, most of the Romanians born after 1980 have the same characteristics regarding their career or life.

The contemporary conflicts challenges are into continuum updating. New technologies are always on the both sides of belligerents. Here is no boundary between civilian and military personnel, the targets diffuse and in the same times very clear reached. Anyone should be the target of the economic war, crisis and social media or just the consumer propaganda. If the aggressions are based on consumerism[8], persuasion and violation of the traditionalism, the targets are already victims; they are prisoners into their own houses.

---

spontaneously take up arms to resist the invading forces, without having had time to form themselves into regular armed units, provided they carry arms openly and respect the laws and customs of war. B. The following shall likewise be treated as prisoners of war under the present Convention: (1) Persons belonging, or having belonged, to the armed forces of the occupied country, if the occupying Power considers it necessary by reason of such allegiance to intern them, even though it has originally liberated them while hostilities were going on outside the territory it occupies, in particular where such persons have made an unsuccessful attempt to rejoin the armed forces to which they belong and which are engaged in combat, or where they fail to comply with a summons made to them with a view to internment. Art 5. Should any doubt arise as to whether persons, having committed a belligerent act and having fallen into the hands of the enemy, belong to any of the categories enumerated in Article 4.

[7]Vladimir Volkof, *Tratat de Dezinformare*, Editura Antet, translated by Mihnea Columbeanu, De la Calul Troian la Internet, available online at: https://volkoff.mercer.edu/ accessed on 06.10.2014, 15:15 hours.

[8] Consumption and Consumerism by Anup Shah available online at: http://www.globalissues.org/issue/235/ consumption -and-consumerism accessed on 06.10.2014, 15:00 hours.

Into the modern and recent war, the real military forces are not the one who enforces the law or conducting the war. The most important direct actions, during the armed conflicts and not only are the main duties of the private military companies. They might be assimilated to the legal combatants of the globalist but who is the global institution who are punishing them if they are making mistakes? Almost all the private military company who acts in the conflict areas is the contract partners of the United State Department of Defense, United Nations or some nongovernmental organizations. Its members are former military personnel; they know sometimes better then military forces the international law principle and customs. In my opinion, they always behave into the spirit to accomplish those missions. If they are involved into any abuse[9] they always call out the military necessity principle in opposition with the humanitarian law one.

If we are counting those issues, the following core questions might arise:

1. If the civilian personnel who fight against troops have the benefit of the POW status, the world population who are into the poverty and global crisis should enjoy of the protection like the prisoners of the economical war, during the current global economic war for resources?

A proper protection against the poverty should be applied starting with a proper education and propaganda for the rational culture and life.

2. Are all the targets and the victims of the mass media war, and undercover PSYOPS, materialized into the consumerism current and propaganda thoughts out the internet socializations site, allowed to enjoy the status of POW?

Yes, they might be protected by the international law against the mass media persuations on consumerism.

3. Are the unlawfully combatants unlawful for all parts? Should they be protected? Yes, they are human being and should enjoy the human rights protection anyway.

4. Is the permanent environmental manmade degradation an act of aggression against whole global population? Should apply the humanitarian law to the environmental perpetrators, like the global company which use the resources without respect for the nature and life?

5. Is the violence and sex or prostitution propaganda on the media and film industry an aggression against the children and adults? Do they might be protected against the brain wash into the spirit to maintain the core value of humanity like family, respect of the human being, children rights?

Of course, anyone can ask, who is the protecting forces? Who is the aggressor and who has to protect those global victims?

Conclusions

From its position of the human rights protector and humanitarian law protection leader, the United Nations, thought-out its countries' representatives and contributors should update the status of the prisoners of war and the Geneva Conventions III and IV, with the express stipulations regarding the human rights and rule of law principle applicable to all the human being directly passively or actively, accidentally or intentionally involved in the armed conflicts.

The global civil population should be protected like the prisoners of war against the war on terror and the economic war, with clear expressions. International convention updating with national alignment laws regarding the psychological protection from the media

[9] James Risen, Before Shooting in Iraq, a Warning on Blackwater, June 29, 2014. http://www.nytimes.com/2014/06/30/us/before-shooting-in-iraq-warning-on-blackwater.html?_r=0, accessed on 17.10. 2014, 16:00 hours.

persuasions' is a must. The self censorship should be enforced in the spirit to protect children and youths regarding the consumerism and just online socializations and life what can be followed by the non human and non adaptations to the real life.

The illegal combatant's concept should be out of date; all human being might enjoy the human treatment and, of course, the status of prisoner or war. The war is global, visible or not, just the victim's voices are sometimes too low, but the tragedy is everywhere, the economic crisis changed into a real war by the media contribution. The protection of the victim should be updated, to be a real one.

Acknowledgement:

This work was possible with the financial support of the Sectoral Operational Programme for Human Resources Development 2007-2013, co-financed by the European Social Fund, under the project number POSDRU/159/1.5/S/138822 with the title ***"Transnational network of integrated management of intelligent doctoral and postdoctoral research in the fields of Military Science, Security and Intelligence, Public order and National Security – Continuous formation programme for elite researchers - "SmartSPODAS"."***

BIBLIOGRAPHY:

1. ELSEA, Jennifer, *Treatment of "Battlefield Detainees" in the War on Terrorism,* updated January 13, 2005, Legislative Attorney American Law Division, Congressional Research Service, The Library of Congress.
2. GREENBERG, Karen J., DRATEL, Joshua L., The *Torture Papers: The Road to Abu Ghraib*, Cambridge University Press, 2005.
3. VOLKOF, Vladimir Tratat De Dezinformare, Editura Antet, Traducere De Mihna Columbeanu, De La Calul Troian La Internet.
4. UN Charter 1945.
5. NATO Treaty, 1949.
6. Geneva Conventions I- IV, 1949.
7. Additional Protocols, 1977.
8. www.un.org.
9. www.nato.int.
10. www.osce.org.
11. http://eu-un.europa.eu.
12. https://www.icrc.org.
13. http://www.ohchr.org.
14. Convention IV respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 18 October 1907.

THE INTERNATIONAL ORGANIZATION INVOLVED IN WAR PRISONERS' PROTECTION

Victoria CHIRILOIU
Captain, legal branch, PhD candidate with "Carol I" National Defence University, Bucharest, Romania.

Abstract: *After the Solferino battle into the international scene spring up the most important social organization, with the purpose to reduce the war horrors, the International Red Cross Committee. The most humanistic personalities of Europe decide to write down the customs and put it on the Enlightenment spirit; The World War I and its horrors comes out with the League of the Nations in 1929, and the Second World War make it the United Nations Organizations. Those organizations are the promoters of the humanitarian law and then the source of it.*

There was no military conflict after 1949 without the United Nations involvement, resolutions or mandate for the peacekeepers. Also UN fights against the most dangerous kind of war, the social problems, the poverty, the discriminations, and the famine. As a global organization, the UN is also leading the local or national organizations who have the same goal.

Keywords: *war, prisoners, status, protection, international, security, organizations.*

Introduction

Human security is the most important humanitarian purpose, the supreme goal. No matter if it concerns the international level, neither the family situation, it was legislated in the Universal Declaration of Human Rights, the milestone document issued by the United Nations Organizations (UN), on December 10, 1948, at the Paris meeting. It was the result of World War II atrocity but its scope is still a necessity today. No matter how educated or rich humanity becomes, the human being is still under the same challenges, the human rights enforcement, especially during the military conflicts when the humanitarian law should come into force. Each combatant can become a prisoner of war and might be under the protection of the Status of the prisoners of war, regarding the Third Geneva Convention in 1949. If we are looking for the law applicable to the human dignity, it must be respected anytime, no matter if it is peacetime or wartime, if we mind the family level or the global level issues.

According with Geneva Conventions, a prisoner of war (PoW) is a combatant or non-combatant person, who was taken prisoner during the military conflict and to whom might be applied at least the same treatment, regarding the accommodations, food, medical facilities, to them own forces[1]. A minimum standard of the *Rules for the treatment of prisoner was issued by the Special Conference of UN on August 30, 1955, approved by the Economic and Social Council by its resolutions 663 C (XXIV) of 31 July 1957 and 2076 (LXII) of 13 May 1977.* This principle might be enforced but the reality on the ground was and is always different.

The international law have also the notion of unlawful combatants, who, in their opinion, are the one which do not respect the combatants code of conduct, the one who are not

[1] Geneva Convention III regarding the Status of the prisoners of war, Geneva, 12 August 1948.

described on the article 4 and 5 of Geneva Convention regarding the Status of Prisoners of War[2]. Those are the mercenaries, the spies, the terrorists and others.

The Article 47 of *Protocol I, Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, explain* clearly *"A mercenary shall not have the right to be a combatant or a prisoner of war"* but this according with the law principle *per a contrario*[3], do not exclude the human rights principle. Only the legal combatant is allowed to enjoy the privileges of the status as prisoner of law.

The International Organization Involved into the Prisoners of War Protections

The largest global organizations which are mostly involved into the protection of war prisoners are the United Nations and the International Committee of the Red Cross (ICRC) and Red Crescent Movement (RCM).

The International Committee of the Red Cross is the most important actor in supervising the prisoners of war. Since 1863, the Red Cross was all over the world doing the humanitarian missions, improving the life of the war victims and giving the hope to the people who are lost into the reconstruction post conflict process.

According with their site, the ICRC mandate is strictly under the UN and Geneva Convention and Protocol law. The work of the ICRC is based on the Geneva Conventions of 1949, their Additional Protocols, the Statutes of the International Red Cross and Red Crescent Movement and the resolutions of the International Conferences of the Red Cross and Red Crescent. The ICRC is an independent, neutral organization ensuring humanitarian protection and assistance for victims of war and armed violence. It takes action in response to

[2] Art. 3 and 4, *Convention (III) relative to the Treatment of Prisoners of War,* Geneva, August 12, 1949, provisions: "Prisoners of war, in the sense of the present Convention, are persons belonging to one of the following categories, who have fallen into the prisoners of war of the enemy:
1. Members of the armed forces of a Party to the conflict as well as members of militias or volunteer corps forming part of such armed forces.
2. Members of other militias and members of other volunteer corps, including those of organized resistance movements, belonging to a Party to the conflict and operating in or outside their own territory, even if this territory is occupied, provided that such militias or volunteer corps, including such organized resistance movements, fulfill the following conditions:
(a) That of being commanded by a person responsible for his subordinates;
(b) That of having a fixed distinctive sign recognizable at a distance;
(c) That of carrying arms openly;
(d) That of conducting their operations in accordance with the laws and customs of war.
3. Members of regular armed forces who profess allegiance to a government or an authority not recognized by the Detaining prisoners of war.
4. Persons who accompany the armed forces without actually being members thereof, such as civilian members of military aircraft crews, war correspondents, supply contractors, members of labour units or of services responsible for the welfare of the armed forces, provided that they have received authorization from the armed forces which they accompany, who shall provide them for that purpose with an identity card similar to the annexed model.
5. Members of crews [of civil ships and aircraft], who do not benefit by more favorable treatment under any other provisions of international law.
6. Inhabitants of a non-occupied territory, who on the approach of the enemy spontaneously take up arms to resist the invading forces, without having had time to form themselves into regular armed units, provided they carry arms openly and respect the laws and customs of war".
"The following shall likewise be treated as prisoners of war under the present Convention: 1. Persons belonging, or having belonged, to the armed forces of the occupied country...".
[3] What is not restricted by the law is presumed to be permitted.

emergencies and promotes respect for international humanitarian law and its implementation in national law[4].

During the international armed conflicts, Geneva Conventions III, article 126 and Geneva Conventions IV, article 143 give express competence to the ICRC to visit detentions centers. Moreover, the ICRC personnel are allowed to visit any detentions place and have meetings with the detainees without any witness. Since October 1990, the UN General Assembly invited the ICRC to take part in its proceedings as observers.

1. The United Nations (UN) Role in the Protection of the Prisoners of War

The UN was the actor that initiates the Geneva Conventions acting in the spirit of humanity and international human rights. One of the Conventions, Geneva III, expressly establishes the Statute of prisoners of war. Protection of the prisoners of war was always a main duty for the UN mission. Throughout the International Red Cross or just by the UN personnel, the negotiation regarding prisoners' of war exchange has been something usual during the military conflicts. Protecting human rights or the rule of law is included also in the UN Charter.[5]

According to the UN site, www.un.org, on July 31, 2014, the UN workforces supported by 122 countries contributions of military and police personnel was made from 83,327 serving troops and military observers, and 11,420 police personnel. The number of the entire UN civilian personnel was 5,233 international civilian personnel, completed with 11,954 local civilian staff and 1,798 UN volunteers. UN does not have its own military force, its forces base on the contributions from the Member States.

At present, UN has peacekeeping mission from Afghanistan to Haiti and Africa, and also a large number of military observers. The most important UN mission is peacekeeping, with an essential role into the postconflict reconstruction and the new peace establishment.

Exchanging the war prisoners are a today practice in Ukraine 2014 conflict, according with *Autonomous non-profit organization (ANO) "TV-Novosti", Channel "RT TV", "The exchange has taken place,"* a representative of the DPR's defense ministry told Interfax earlier. "We handed 36 prisoners over to the Kiev side in exchange for 31 of our supporters. Kiev promises to hand over five more tomorrow."[6]

The Office of the United Nations High Commissioner for Human Right sent to Ukraine a Human Rights Monitoring Mission to monitor the human rights situation and to provide support to the Government and local organizations. UN was always involved into the protection of prisoners of war; there is no mandate or resolution of Security Council where the matter of the human rights and prisoners status had been omitted. One of the examples is when the UN Security Council made the Presidential statement regarding the releasing of the prisoners of war from Etiopia and Eritrea, on 2000. The issues update with the Resolution of Security Council number 1359 from 2001 and the Security Council call SC/7255 from 2002, with focus on the protection of the prisoners of war of Western Sahara.

During the Iran – Iraq War the UN Security Council adopted Resolution 552 in 1984 requiring all the countries of the region to contribute to the peace and release the prisoners of war from both countries.

---

[4] International Committee of the Red Cross, *Mandate and Mission,* https://www.icrc.org/en/who-we-are/mandate, accessed on 28th of September 2014, 21:00hours

[5] The Charter of the United Nations was signed on 26 June 1945, in San Francisco, at the conclusion of the United Nations Conference on International Organization, and came into force on 24 October 1945. The Statute of the International Court of Justice is an integral part of the Charter. http://www.un.org/en/documents/charter/preamble.shtml accessed of 17.10.2014, 15:20 hours

[6] Autonomous non-profit organization (ANO) "TV-Novosti", Channel "RT TV"http://rt.com/news/187120-ukraine-militias-prisoner-exchange/ site accessed on 17.10.2014, 15:35 hours

2. European Union, NATO and OSCE

As a regional political organization, EU is stressed on the human rights and rule of law implementations. The Council of Europe adopts the European Convention for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment at Strasbourg, 26.XI.1987. It should be applied to any situations and everywhere. EU politics is always focusing on human rights and international law and its legislation is into concordance with the UN resolutions and legal publications. Of course, the core of EU external policy regarding human rights, during the armed conflict and not only, is the commitment of the UN goals, like the strengthening of the UN and humanitarian system, promoting the human rights, democracy and rule of law, what into the large area obviously means protecting the prisoners of war and their status. It is also important to say that two of the permanent members of UN Security Council are also EU members, France and the United Kingdom.

Regarding EU prisoners of war status protection, an example is the Resolution of European Parliament regarding the Palestinian prisoners of war situated into the Israeli prisons, issued on 8 of September 2008. The EU has been asked the Israel to respect the status of the prisoners of war in any circumstances.[7]

The European Organization for Security and Co-operation in Europe is called OSCE. It is the most important regional actor for Europe and West Asia and not only working in cooperation with UN and NATO. OSCE acts to prevent arising of new conflicts and to facilitate the lasting of comprehensive political settlements for the existing conflicts. It also helps with the process of rehabilitation in post-conflict areas. It cooperates with representatives of the United Nations and other international organizations operating in areas of conflict.[89i] OSCE observers during the Ukraine and Russia conflict from summer 2014 had a key role into the prisoners of war exchange and monitoring of human rights.

OSCE, based on Vienna Treaty on Conventional Armed Forces in Europe from 1990, with a main role to maintain balance between the NATO and Warsaw Organization, was growing up with a large area of security components, from the population affairs to the armed control and environmental issues[10]. Right now, the organization has an important role into the Ukraine regional conflict, monitoring and mediating the situation.

North-Atlantic Treaty Organization (NATO) is the most important military and political organization and its main purpose is collective defense. The Article 5 of the NATO Treaty expresses the collective defense principle to be the extension of the article 51 of UN Chart. Those institutions have many common goals but we have to mention that UN is an international security organization and NATO is a regional military and political organization. Some differences might arise from their specific interests and missions.

NATO has its special standard operation procedure regarding prisoners of war treatments, based on Geneva Conventions and in the spirit of the international humanitarian law. STANAG 2033, *Interrogation of Prisoners of War (PW) (Edition 6),* December 6, 1994 and STANAG 2044*, Procedures for Dealing with Prisoners of War (PoWs) (Edition 5)*, in June 28, 1994. Since those documents are classified, we cannot comment and debate on it. According to NATO Treaty Preamble, 'The Parties to this Treaty reaffirm their faith in the

[7] Résolution du Parlement européen du 4 septembre 2008 sur la situation des prisonniers palestiniens dans les prisons israéliennes, available online at: http://www.palestine-solidarite.org/ressources.parlement-europeen. 040908.htm accessed on 30.09.2014, 16:00 hours .

[8]The European Union at the 69th UN General Assemblyhttp://euun.europa.eu/articles/en/article_15485_en.htm, accessed on 29. 09. 2014, 15:00 hours

[9] The OSCE works to prevent conflicts from arising and to facilitate lasting comprehensive political settlements for existing conflicts http://www.osce.org/what/conflict-prevention accessed on 29. 09. 2014, 15:006 hours.

[10] The OSCE's comprehensive view of security covers three "dimensions": the politico-military; the economic and environmental; and the human, http://www.osce.org/what, accessed on 29. 09. 2014.

purposes and principles of the Charter of the United Nations and their desire to live in peace with all peoples and all governments. They are determined to safeguard the freedom, common heritage and civilization of their peoples, founded on the principles of democracy, individual liberty and the rule of law. They seek to promote stability and well-being in the North Atlantic area. They are resolved to unite their efforts for collective defence and for the preservation of peace and security. They therefore agree to this North Atlantic Treaty'.

So, for the best goal with the best tools, should be the right way of NATO policy. Moreover, starting with the Lisbon Summit, NATO became more proactive and predictive in the fight against terrorism but the 2003/2004 history from NATO members country, US, Abu Graib Iraqi detention centre shows up that the errors and misunderstanding generated huge violation of prisoners of war status and Geneva conventions and Protocols.

In our opinion, if we are looking at the issues related to the *Enemy prisoners of War*, common fact of US and UK, we can find a rapid a logical explanation for the horrible phenomena happened in Iraq in 2003 and 2004. But, where are the human rights, the respect for the human being and rule of law? The international humanitarian law does not have such terms as prisoners of war and enemy prisoner of war. No matter they are humanly treated or not, they are human beings and first of all, anyone should be presumed of innocence until the evidence demonstrates de truth.

Later, after the genocide of Bosnia and Rwanda, UN focused on the application of the status of prisoners of war to the civilian population, especially to the women and children, including the rape and sexual violence in the crimes against humanity category, according with UN Resolution 1820 (2008). Its call on reducing sexual violence and bringing the perpetrators to law will have to be gauged in places such as the Democratic Republic of Congo (DRC)—arguably the epicenter of sexual violence against women today—as well as Liberia and the Darfur region of Sudan[11].

3. Local Organization Responsible for the Protection of Prisoners

In Israel, generally, The Public Committee against Torture is the local organization responsible for the protection of prisoners and also includes the prisoners of war[12]. The most important documents for our research is "No Defence: Soldier Violence against Palestinian Detainees" Report *issued in* June 2008 that exposed the widespread phenomenon of violence by Israeli soldiers against bound Palestinian detainees, who no longer present a danger to the arresting forces. It shows that phenomenon is exacerbated by the almost absolute indifference of the authorities and a weak law enforcement system which rarely investigates complaints or brings perpetrators to justice[13].

In Europe, Amnesty International was founded by British lawyer Peter Benenson after hearing about two Portuguese students imprisoned for speaking about freedom in 1961. In present, the nongovernmental organization has branches into many countries. The representatives of Amnesty International are very persuading opinion leaders with active voice into the international and local media.

---

[11] ***UN Human rights institute,*** **Rape: Weapon of war*, available online at: http://www.ohchr.org/en/newsevents/ pages/rapeweaponwar.aspx, accessed on 15.10.2014, 12:00 hours***

[12] The Public Committee Against Torture in Israel (PCATI), http://www.stoptorture.org.il/en/atirot, accessed on 10.10.2014, 10:00 hours.

[13] *The UN work on Palestine,* available online at: http://www.un.org/depts/dpa/qpal/docs/2012%20Geneva/ P2%20Y aser%20Amouri%20EN%20revised%20.pdf.

[14]DOSSIER Prisonniers Palestiniens, available online at: http://www.palestinesolidarite.org /dossier.prisonniers_ palestiniens. rapport.100406.htm accessed on 12.10.2014, 11.00 hours.

Conclusions

UN is the most important international actor in the humanitarian affairs field as international security organizations, with 193 country members, especially in concern to the prisoners of war protections. The Security Council resolutions give the mandate to involve in the most of the conflicts after the fall of the Iron Curtain, and also by their observers or by the ICRC reports supervises the implementations of the rule of law and the preservation of the prisoners of war status.

Since 1863, the Red Cross and later the ICRC generated and maintained de humanitarian movement with palpable results of persuasion over the political opinion of the world leaders, who later, came together first in the League of the Nations, in 1929, and later, in 1945, in the UN. No latter, in 1948 and 1949, UN wrote down the most important legislation regarding humanitarian issues, especially the Status of the Prisoners of War.

Today, both organizations are looking for the human rights preservation during the crisis and military conflicts. They are the last hope for the people being in extreme situations. UN reputation, built in cooperation with ICRC, is the most important guardant of prisoners of war status application.

Acknowledgement:

This work was possible with the financial support of the Sectoral Operational Programme for Human Resources Development 2007-2013, co-financed by the European Social Fund, under the project number POSDRU/159/1.5/S/138822 with the title ***"Transnational network of integrated management of intelligent doctoral and postdoctoral research in the fields of Military Science, Security and Intelligence, Public order and National Security – Continuous formation programme for elite researchers - "SmartSPODAS"."***

BIBLIOGRAPHY:

1. UN Charter 1945
2. NATO Treaty, 1949
3. Geneva Conventions I- IV, 1949
4. Additional Protocols, 1977
5. www.un.org
6. www.nato.int
7. www.osce.org
8. http://eu-un.europa.eu
9. www.icrc.org
10. www.ohchr.org.

THE ADMINISTRATIVE COMMISSION FOR THE COORDINATION OF SOCIAL SECURITY SYSTEMS, THE CONCILIATION BOARD – REGULATION, IMPORTANCE AND IMPACT IN RELATION TO INTERNATIONAL LAW AND COMMUNITY LAW

Dana-Silvia CONTINEANU
Legal expert at ANT, PhD student in Sociology within The Research Institute for Quality of Life, Phd student in Military Scences within "Carol I" National Defence University, Bucharest, Romania.
E-mail address: dscconti@yahoo.com

Abstract: *In this paper we intend to present the role, importance and impact of the Administrative Commission for the Coordination of Social Security Systems and the Conciliation Board in relation to the international law and community law. In this framework of our paper, we notice that the free movement of citizens on European Union territory has been generated for them not only benefits and rights, but also obligations for them and the necessity of a better coordination of social security systems of the member states. This is the way of creating the Administrative Commission for the Coordination of Social Security Systems and the Conciliation Board. These two entities are functional levers of the European Commission and ways of achieving a coherent coordination of social security within EU, identifying vulnerabilities of social security and also solving some state differences regarding the way of application and interpreting the Regulation (EC) No 883/2004 of the European Parliament and of the Council on the coordination of social security systems and Regulation (EC) No 987/2009 of the European Parliament and of the Council laying down the procedure for implementing Regulation (EC) No 883/2004. We can consider these levers as concrete ways of managing the migration of labor and assuring a concrete social security for EU citizens.*

Keywords: *The Administrative Commission for the Coordination of Social Security Systems, Conciliation Board, coordination of social security, free movement.*

1. The rules of international law, of community law and national law – general aspects

Throughout history, the humanity has found the need to adopt common rules on a global and regional level so that certain issues or disputes to be settled or legal regulated more efficiently, and to prevent conflicts between states. Thus the agreement of the states was materialized by legal means such as the treaty and customary law and this how the international law appeared. More broadly, international law is the body of legal rules governing the relations that are established in the international society.

At present, according to the American Society of International Law, "International law is traditionally defined as the law between sovereign nation-states, hereinafter, states, especially within the context of the laws of war, peace and security, and protection of territories. While these concerns of international law remain paramount among states today, the classic definition of public international law has expanded to include a more diverse group of subjects and a broader scope of activities.

In addition to states as subjects of international law, other participants engaged in international law activities and its development include private entities, individuals, and international organizations."[1]

In developing rules of international law, there are not responsible legislative bodies nor higher than the states. In the international legal order, the state is simultaneously the author and recipient of the rule of international law. For this reason, the international law is considered coordination law[2].

In international law there is no government authority to pursue the enforcement of rules and no system of judicial bodies to ensure the compliance control.

Court of Justice of European Union has established, by jurisprudence, that existing treaties concluded by the European Community, which contain provisions directly applicable, take precedence over EU rules (prior or subsequent treaties concerned), which in this case are inapplicable. The treaties concluded by the European Community and in force, take precedence over the national law of the Member States of the European Union and have direct effect over their legal rules.

The community law is defined by some authors as "a legal order derived from international" (G. Sperduti)[3]. The European Communities are the result of the conclusion of treaties between sovereign states (constitutive treaties). The community law contains mainly the Treaties which are establishing the European Communities, the amending treaties, the decisions and accession treaties, the Treaty of Maastricht, Treaty of Amsterdam, Treaty of Nice, the decisions of Communities' own resources and others, but alos the rules adopted by the Community's institutions for the purposes of application of the Treaty, such as regulations, directives, decisions. The rules adopted by the Community institutions have legal binding for Member States[4].

To the features mentioned above briefly, we can say that the similarities and differences between the international law and the EU law derives primarily from the proportion of the Community law and national law.

Thus, the opinion 1/91 of 14 December 1991 of the Court of Justice of European Union decided that the Community rule overrides any other national rule, with immediate applicability.

2. The free movement of citizens and social security within European Union

In international relations, the free movement of citizens has limits and clear rules to respect state borders and national laws, and in some cases social and cultural differences. In case of the free movement of workers, worldwide, may conclude bilateral agreements between states in a way so their social rights can be respected. An example is our country, where in the past years, social security agreements were concluded with Moldova, Republic of Macedonia, Turkey, Israel. In the European Union, however, the right of persons to free movement has to be accompanied by social security measures so that the common market objectives are respected.

The right of EU citizens to freely move to and live in any EU country, along with their family members, is one of the four fundamental freedoms enshrined in EU law and a cornerstone of EU integration.

---

[1] http://www.asil.org/sites/default/files/ERG_PUBLIC_INT.pdf.

[2] *Raluca Miga – Beşteliu,* Drept internaţional. Introducere în dreptul internaţional public, ediţia a III-a, Editura ALL Beck, 2003.

[3] A. Năstase, B. Aurescu, C. Jura, *Drept Internaţional public Sinteze pentru examen ,* ediţia 4, Editura C.H. Beck, Bucureşti, 2006.

[4] Octavian Manolache, *Tratat de drept comunitar,* ediţia 5, Editura C.H.Beck, Bucureşti, 2006.

EU workers have benefited from this freedom since the 1960s[5]. With the Treaty of Maastricht the right to free movement was recognised for all EU citizens, whether they are economically active or not. Since then, being able to move freely for purposes other than working, for instance to retire, study or accompany family, has become an essential feature of EU citizenship.[6]

Thus, initially were adopted and applied to the European Union, the first regulations on social security, namely Regulations nos. 3/1958 and 4/1958. Later on, they were replaced by Regulation (EEC) no. 1408/71 on the application of social security schemes to employed persons and their families moving within the Community and Regulation (EEC) no. 574/72 which covers the practical implementation. As the EU expanded with new member states and the geographical development of exercising the right to free movement, there was a need to develop new rules updated in line with new challenges concerning the improving of living standards and the conditions of employment of people.

Following this, the European Parliament and Council adopted Regulation (EC) no. 883/2004 on the coordination of social security systems, called the basic Regulation and Regulation (EC) no. 987/2009 laying down the procedure for implementing Regulation (EC) no. 883/2004 also known as the implementing Regulation.

And so, there is a mechanism for the coordination of social security systems which is not only new legal rules but they are also adapted to the new situations arising in social security, based on the experience of Member States during the implementation of the old regulations.

3. The Administrative Commission for the Coordination of Social Security Systems and the Conciliation Council

The provisions of article 71 „Composition and working methods of the Administrative Commission" rules the members of this commission and how it works.

The Administrative Commision for the Coordination of Social Security Systems, called shortly as ''the Administrative Commission" is attached to the Commission of the European Communities. It is made up of a government representative from each of the Member States, assisted by expert advisers, where necessary. A representative of the Commission of the European Communities shall attend the meetings of the Administrative Commission in advisory capacity.

The Administrative Commission shall activate by the rules drawn up by mutual agreement among its members. Decisions on matters of interpretation concerning its legal tasks, shall be adopted under the voting rules established by the Treaty and shall be given the necessary publicity.

The Commission of the European Communities shall provide the secretarial services for the Administrative Commission.

According to the article 72 of the basic Regulation, „the Administrative Commission shall:

(a) deal with all administrative questions and questions of interpretation arising from the provisions of this Regulation or those of the Implementing Regulation, or from any agreement concluded or arrangement made thereunder, without prejudice to the right of the authorities, institutions and persons concerned to have recourse to the procedures and tribunals provided for by the legislation of the Member States, by this Regulation or by the Treaty;

(b) facilitate the uniform application of Community law, especially by promoting

[5] Art. 45 and 48 of the Treaty on the Functioning of the European Union (TFEU).
[6] Art. 21 TFEU

exchange of experience and best administrative practices;

(c) foster and develop cooperation between Member States and their institutions in social security matters in order, inter alia, to take into account particular questions regarding certain categories of persons; facilitate realisation of actions of crossborder cooperation activities in the area of the coordination of social security systems;

(d) encourage as far as possible the use of new technologies in order to facilitate the free movement of persons, in particular by modernising procedures for exchanging information and adapting the information flow between institutions for the purposes of exchange by electronic means, taking account of the development of data processing in each Member State; the Administrative Commission shall adopt the common structural rules for data processing services, in particular on security and the use of standards, and shall lay down provisions for the operation of the common part of those services;

(e) undertake any other function falling within its competence under this Regulation and the Implementing Regulation or any agreement or arrangement concluded thereunder;

(f) make any relevant proposals to the Commission of the European Communities concerning the coordination of social security schemes, with a view to improving and modernising the Community "acquis" by drafting subsequent Regulations or by means of other instruments provided for by the Treaty;

(g) establish the factors to be taken into account for drawing up accounts relating to the costs to be borne by the institutions of the Member States under this Regulation and to adopt the annual accounts between those institutions, based on the report of the Audit Board referred to in Article 74."[7]

In the Official Journal of the European Union, 2010/C 213/11 were published the Rules of the Administrative Commission for the Coordination of Social Security Systems attached to the European Commission. Article 1 of the Rules says that ''The Administrative Commission is a specialised body of the European Commission and has the same seat". The office of the Chair of the Administrative Commission shall be held by the member belonging to the State whose representative to the Council of the EU holds the office of the President of the Council of the EU for the same period. The Administrative Commission may set up an Operational Board to assist and facilitate its work. It may set up working parties or study groups for special problems. These working parties and study groups shall be presided by a person designated by the Chair of the Administrative Commission in consultation with the representative of the European Commission. The working parties shall have a mandate to carry out its tasks in a way that findings can be accepted by the Administrative Commission without further deliberations. Also, the Administrative Commission may set up ad-hoc groups, with a limited number of persons to prepare and present to this Commission proposals for adoption on specific issues. We may say that there were ad-hoc groups on habitual residence test, on combating fraud and error, on long-term care etc.

The Administrative Commission meets at least four times a year. Every meeting has an agenda where are subjects proposed by the Secretary General in consultation with the Chair of the Administrative Commission and the representative of the European Commission. At the beginning of each meeting, the agenda shall be approved by the Administrative Commission.

The decisions of the the Administrative Commission shall be published in the Official Journal of the European Union and shall apply from the date specified therein or, if no such date is mentioned from the first day of the second month following its publication in the Official Journal.

[7] Regulation (EC) no 883/2004 on the coordination of social security systems.

For each meeting of the Administrative Commission minutes are recorded which are, in principle, to be approved at the following meeting. It shall periodically draw up a general report on its activities and on the implementation of the regulations on the coordination of social security systems. Where the provisions of these rules require interpretation, such interpretation shall be given by the Court of Justice of the European Union in accordance with the Article 267 of the Treaty on the Functioning of the European Union. We believe that this is the most important mechanism on the coordination of the social security systems.

According the article 5 of the Rules, the Administrative Commission may set up a Conciliation Board to assist its work in case of differing interpretation between members with the provision of Regulation (EC) no 883/2004 and Regulation (EC) no 987/2009. The details of the composition, term, tasks, working methods as well as the system of Chairmanship of the Conciliation Board shall be contained in a mandate decided upon by the Administrative Commission. Its functioning shall be reviewed on a regular basis.

In 2009 the Conciliation Board was constituted in accordance with its mandate laid down in Note CA.SS.TM. 553/09REV approved at the 318th meeting of the Administrative Commission on 16-17 December 2009.

The Conciliation Board held a first plenary meeting on 4 October 2010 and decided to propose to the Administrative Commission to approve the system of chairmanship and the subdivision of the members. The Administrative Commission adopted these proposals at its 323rd meeting on 20-21 October 2010.

According to the adopted mandate at the 318th meeting of the Administrative Commission on 16-17 December 2009, the objective of the Conciliation Board is, upon request, to reconcile differing interpretations between members of the Administrative Commission arising from provisions of the Regulations and, if also requested, to provide it with a legal opinion on such issues.

The Conciliation Board shall consist of a maximum of 12 volunteers nominated by national Administrative Commission delegations and appointed by the Administrative Commission for a term of 24 months. The members of the Conciliation Board shall not act as members of their delegation, but shall act on the basis of their personal expertise in an impartial manner. A member of the Conciliation Board shall abstain from any work on an issue which concerns his or her country of origin or when his or her impartiality could be compromised in any other way.

The Conciliation Board shall work in a system of 3-4 groups, composed of 3-4 members and a Commission representative each, taking account of the experience of members in certain sectors and with certain national social security systems. The subgroups of the Conciliation Board are:

- Applicable Legislation;
- Sickness Maternity and Equivalent Paternity Benefits; Benefits for Accidents at Work and Occupational Diseases;
- All Other Sectors.

For the first time, in 2013, Romania had a member in the Conciliation Board.

All legal opinions of the Conciliation Board shall be drafted by consensus. If there can be no consensus reached on a certain issue, the minority view has to be stated clearly in the Opinion submitted to the Administrative Commission. The Chair of the Conciliation Board shall report to the Administrative Commission at least once year in writting on its activities.

Conclusions

The Administrative Commission analyzes and proposes rules on the external dimension of EU social security and thus it appears tangents about the rules of international

law. This means that Member States can sign treaties with non-member States in social security field but they must respect the general legal framework established by the Administrative Commission. Given its institutional powers presented in this paper, we consider that there is an interaction between the interpretation of international conventions and applicable social security legislation for workers of international staff of various international organizations such as NATO, the European Commission etc. In this case, if a worker is subject to compuslory insurance by virtue of the legislation of his Member State, he may not be subject to a voluntary insurance scheme or an optional continued insurance scheme in another Member State. But, he can make his choice without leaving the social security system from his Member State. So, a person working for International Staff in NATO, even he has a several voluntary insurance scheme or optional continued insurance scheme, he must remain insured in the social security system in order to get the benefits regulated by the Regulation (EC) nos 883/2004 and 987/2009.

We may say that these rules does not exclude each other and there is a need to know the mechanisms so that the coordination of social security systems does not affect the social rights of the insured persons

The Administrative Commission and the Conciliation Board are concrete ways of managing the migration of labor and assuring a concrete social security for EU citizens in such way to protect and develop the free movement of the EU citizens.

Acknowledgement:

This paper is made and published under the aegis of the Research Institute for Quality of Life, Romanian Academy as a part of programme co-funded by the European Union within the Operational Sectorial Programme for Human Resources Development through the project for ***Pluri and interdisciplinary in doctoral and post-doctoral programmes*** Project Code: POSDRU/159/1.5/S/141086

Sectoral Operational Programme Human Resources Development 2007-2013

Project Title: Pluri and interdisciplinarity in doctoral and post-doctoral programmes

Editor of material:

Date of publication:

The contents of this material do not necessarily represent the official position of the European Union or the Romanian Government.

BIBLIOGRAPHY:

1. MANOLACHE, Octavian, Tratat de drept comunitar, ediţia 5, Editura C.H.Beck, Bucureşti, 2006.
2. MIGA-BEŞTELIU, Raluca, Drept internaţional. Introducere în dreptul internaţional public, ediţia a III-a, Editura ALL Beck, 2003.
3. NĂSTASE, A.; AURESCU B.; JURA C., Drept Internaţional public Sinteze pentru examen, ediţia 4, Editura C.H. Beck, Bucureşti, 2006.
4. Treaty on the Functioning of the European Union (TFEU).
5. Official Journal of the European Union, 2010/C 213/11.
6. Note CA.SS.TM. 553/09REV.
7. Regulation (EC) no. 883/2004 on the coordination of social security systems.
8. Regulation (EC) no. 987/2009 laying down the procedure for implementing Regulation (EC) no. 883/2004.
9. American Society of International Law http://www.asil.org/sites/default/files/ERG _PUBLIC_INT.pdf.

ENERGY SECURITY OF LARGEST GLOBAL CONSUMERS – MAIN THREAT FOR THE GLOBAL SECURITY

Cristina TEODORESCU
PhD, Director at Vimetco Management Romania

Abstract: *China replaced 2010 the United States as largest global energy consumer, while in 2014 it became also the main crude importer worldwide – the same ranking as in the case of the largest armies. Fuelling the economies – but also the armies – represents one of the most important, if not the main objective of any government But the world's energy resources are not only permanently decreasing, they are also pretty scarce. Back in 2007, the unanimously accepted predictions were: 40 years of petrol and as many for uranium, 70 for gas and 130 for coal. Since then, the reserves are falling and no important discovery has been announced. Under these circumstances, it is not farfetched to predict that the ongoing conflicts, from the Middle East to Ukraine, are only a prelude to what is going to come.*

Keywords: *Energy resources, oil, armies, conflicts, energy security, global security*.

Introduction

The theoretical linkage between the scarcities of different types of resources - needed by manhood in order to live in a convenient way - and different degrees of insecurity is almost as old as the phenomenon itself. The beginning was made by the battle for food in the prehistoric era, while for the almost on the date last 100 years we are facing a fierce battle over energy resources and foremost over oil[1)]. Given the case, it is of interest for any security scientist to try at least to predict where the conflicts of the future are going to hit and which will be their trigger. While working on the subject, the conclusion was surprising, even shocking. Due to the fact that on a close look the thesis of the renewable energy resources as a safe alternative to the fossil fuels proves to be nothing more than a very clever marketing lie, it is rather clear that before fighting over water – the general thesis that the conflicts of tomorrow are going to be about – people will have to continue to fight mainly over fossils, mainly over oil and natural gas. And at the end of this fight, for the moment, nothing else can be predicted except a very painful return into a very far past.

Every consumer will be forced to do everything in his power to satisfy its own need for energy. Every head of state and implicitly of an army will have to do everything in his power to satisfy the need for energy of its own folks, because otherwise he will be confronted with a very serious threat of insecurity, maybe the most powerful of all – the threat of his own people rioting against himself and his power. For the leader himself that would be the end of his career but possibly also of his life, for his people, that would be the end of an era of peace and prosperity, but also, in the worst case scenario, it could be the end of its state altogether. It is a lesson of the year 1989 what the force of people rising against their own leaders can have as a result: not only that head of states where falling one after the other – in the Romanian case the expression has to be taken literarily -, not only that many of their states where confronted with inner disorder peaking with some of them thrown into inner war, but even the

[1] F. William ENGDAHL, *Mit der ölwaffe zur Weltmach – Der Weg zur neuen Weltordnung*, Rottenburg, Jochen Kopp Verlag, 2006, p. 13.

world order was shaken from roots on, as some of its social systems - such as socialism, apartheid or the military dictatorships in South America – vanished from one day to the next as if they would have never existed.

1. Progress and development of increasing population multiply energy consumption

In the following paragraphs we will present figures and facts to support our theory that the world as we know it today really reached its limits. Of course, this article is not meant to repeat warnings already made long time ago. Over four decades ago by Marion King Hubbert, whose peak-oil-theory[2] proved as correct as soon as the first oil crisis begun in the1970s, then in 1972 by Donella H. Meadows, Dennis L. Meadows, Jørgen Randers and William W. Behrens III in their so disputed *The Limits of Growth*[3], not to mention the spiritual father of people being aware of overpopulating a planet with lots of resources which are not renewable - Thomas Robert Malthus with his *An Essay on the Principle of Population*[4], written already back in 1798. We are much more aiming to link these facts to the current security situation of the world, explaining it from the angle of the resource scarcity. Even this approach isn't singular, but it isn't common knowledge either, so due to the seriousness of the subject, presenting it again to new readers can be only of help.

We chose to exemplify our point of view with charts and figures prepared both by the biggest Western oil companies, as well as by Russian state run research organizations. Due to the linkage between Western oil companies and decision takers in their countries of origin – the connection of former US VP Dick Chenney and Halliburton is as well known, as the lobbying of the retired US General Wesley Clark, nowadays also adviser to the Romanian PM Victor Ponta, for the shell oil and mining in general[5]. By choosing information accessible to the leaders of the two blocks involved in the former and the new cold war of the geopolitics we want to underline that the facts are well-known in every decision maker office all over the globe. And that due to these figures, facts and realities, these leaders should be confronted with inner conflicts going back to the fact that they have to choose between the backdrop and impoverishment of their own folks, due to constantly fewer – even if not (yet) constantly more expensive – energy resources and a return to conflict and force in order to insure for themselves and their people energy resources meant to help keeping the existing status quo for as long as possible. And not only for their time in office, because they do not represent only themselves, but also organizations such as parties, intelligence services or simply patriotic feelings and their country's interests. In the end of our essay we will come to the conclusion that they made their decision in this inner conflict they should be confronted with.

In figure 1, we can observe the huge increase in energy consumption during the last century. It is obvious that the steepest jump in progress and comfort realized by manhood in its entire history is represented by the period of relative peace and peaking energy consumption starting with the end of WWII. Same time we have to notice that the increase we are looking at does not reflect also the period of fantastic industrial and economic development of China, so that for the period between 2000 and at time we have to expect

---

[2] Hubbert M. KING, *Nuclear Energy and the Fossil Fuels* http://www.hubbertpeak.com/hubbert/1956/1956.pdf

[3] Donella H. MEADOWS, Dennis L. MEADOWS, Jørgen Randers and William W. Behrens III, *The Limits of Growth* ISBN 0-87663-918-X, 1974 second edition (paperback).

[4] Thomas MALTHUS, *An Essay on the Principle of Population - An Essay on the Principle of Population, as it Affects the Future Improvement of Society with Remarks on the Speculations of Mr. Godwin, M. Condorcet, and Other Writers*, London, Printed for J. Johnson, in St. Paul's Church-Yard, 1798 http://www.esp.org/books/malthus/population/malthus.pdf.

[5] http://www.cotidianul.ro/dupa-kosovo-consilierul-american-al-lui-ponta-e-interesat-de-minerit-in-romania-224772.

even steeper increase rates. We cannot end our comments on the realities reflected in this chart without drawing the reader's attention on two specific colors, namely purple for oil and turquoise for gas. It is obvious that the increase in case of the so non-renewable fossils were the most impressive ones, as well as that they are also the most used ones.

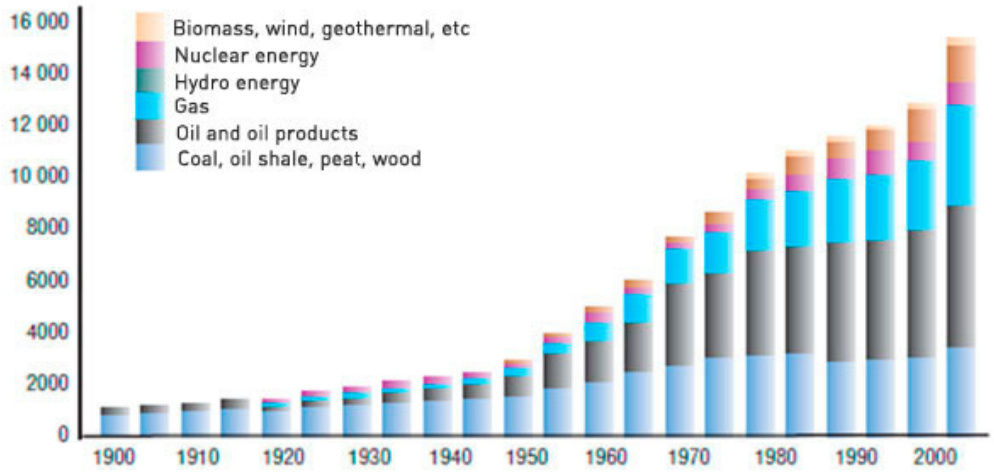


Figure no. 1. Dynamics of world energy consumption in the XX century, mln tons of equivalent fuel[6]

Now to the overlapping of population increase and usage of energy resources, as presented in figure no. 2. In fact, in this case the reflected reality is so clear that words are almost unnecessary. Between 1950 and 2000 – the golden era of world peace (as much it is a shame not to think of all local conflicts that took place during this period of time from South East Asia to Africa to the Middle East and even the dark periods of South America, all in all it was a golden era of global peace) – the population boomed. As we can see in the chart, mainly in the under developed or developing part of the world, the so called Third World. But the big problem contained in this chart reveals itself only when we have a look at the next period of 50 years – 2000 to 2050 – in other words, the period of time we are contemporary with at time and the predictions made for it. Another doubling of population – again in emerging countries – and again another doubling of resources to be needed are forecasted. And as it can be observed in small print in the bottom of the chart, the figures and predictions are as official as they might be: the Organization of the United Nations.

[6] *Russia's energy industry. Problems and prospects. – Moscow, Nauka, 2006,* http://russiancouncil.ru/en/inner/?id_4=588#top.

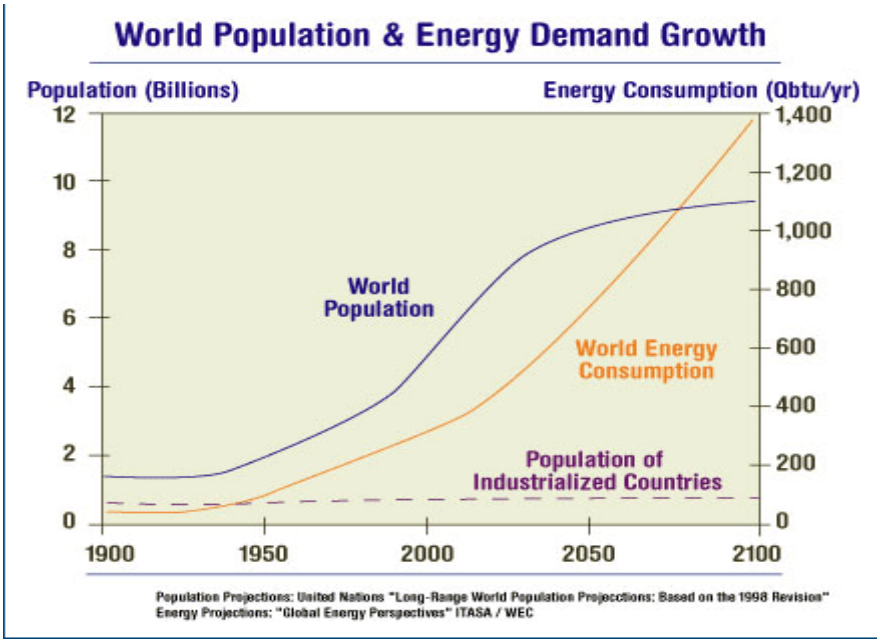


Figure no. 2. The steep increase of population that imposes at least the same increase in finite energy resources[7]

The chart above may be able to answer a lot of questions about the present times and the immediate future, except one: where are the people going to take from those huge amounts of energy resources they are going to need? Knowing the reality of the reserves and confronting it with the reality of demand, only one possible answer is coming to our mind: one from the other. And not in a kind way.

2. Fossil fuels – as scarce as indispensable

To put it plainly: in order to obtain comfort and progress, humans need energy. Lots of it. And what represents now energy, we can see below, in figure 3, which shows which type of resources were and are used, in order to reach today's level of civilization.

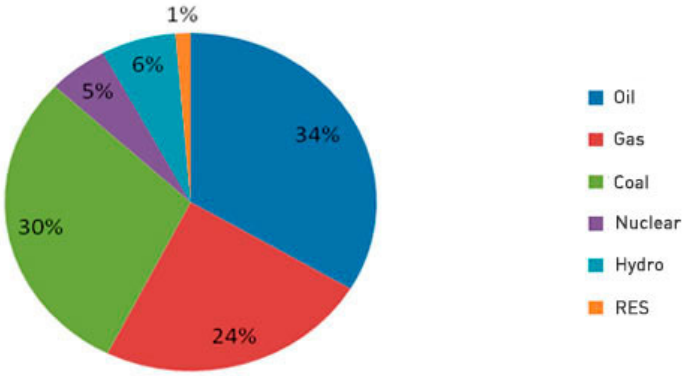


Figure no. 3. Structure of PER consumption in the world, 2011[8]

As we can observe, the largest possible amount of what we do consume are fossils, as non-renewable, polluting – and scarce – they might be. And when we talk nuclear and hydro, we should also think about the tremendous high energy quantities consumed while building a

[7] https://lh4.googleusercontent.com/-FHwzaPzQmSo/TYhT8klhZoI/AAAAAAAABlQ/xz8RkS-khOM/s1600/World-Population-and-Energy.gif , http://pictorial-guide-to-energy.blogspot.ro/p/list-of-charts.html

[8] BP Statistical Review of World Energy, 2011.

hydro or nuclear plant and for how long those so-called green energy providers do have to function in order to make up the 'dirty' part consumed in order to build them. In the case of the modern windmills, it is a fact confirmed to the author by the chief of project at the mill producer Timken: even if a single mutter will not have to be replaced during its lifetime, still the mill wouldn't produce as much energy as used in its production. Talking of green!

As for the near future, the predominant colours will remain, as presented in figure 4, black as oil and dark brown as the coal. The future is dark and not at all bright, even if the so-called renewable will be a little bit better represented. And we never should forget that in the case of the latter we always mean also the subvention money that the producers of 'clean' energy do receive, subventions formed out of money made while using 'dirty' energy.

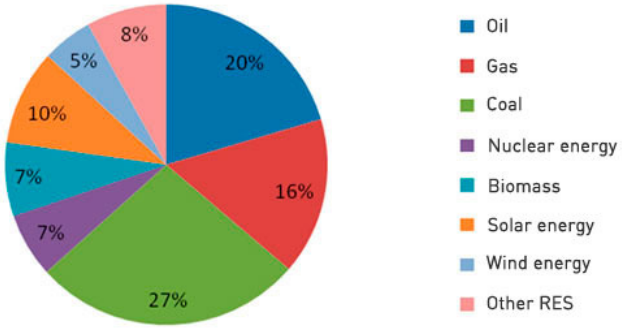


Figure no. 4. Structure of PER consumption in the world, 2050[9]

It is obvious that we are going to need and consume more and more fossil fuels, because neither at time, nor in the predictable future we do not have any sound alternative to them, no matter what the representatives of the 'greens' – a generic term that could be used both for the producers of this type of energy, as well as for the activists fighting against pollution in any form – will have to say against them. Not that pollution wouldn't represent a real matter of concern – in the case of the People's Republic of China we can even speak of an internal security risk, without exaggerating a bit in the process. But especially the crowded China has to choose between two security risks it faces: either letting the people die due to the irrespirable air, polluted by plants fuelled mainly by burning coal – as we can observe in figure 5, China has large reserves of it, but even so, not enough, but on the other hand China also has the highest percentage of lung cancer worldwide due to the burning of coal in order to produce first energy and then progress – or not being able to offer them the progress which means improved standard of life they are longing for and risking to provoke riots among the people.

Figure 5 also shows us how it comes that today we cannot compare the geopolitical situation of the USA and China on one hand and Russia on the other. While the USA and China chase each other in the ranking of the biggest economy worldwide, but also in the list referring to the largest energy consumers of today – both countries are also important producers of energy resources, but in both cases, as much they would produce, it still isn't enough -, Russia has been distributed in another role, a very lonely one.

Russia was, is and will be, for as long its resources will last, the world's real, single energy super-power. It has gas, it has oil and it has coal. And it also has uranium, rivers large enough for both hydro and nuclear plants and a large part of the country covered by forests, too good to be burned down for heating. This plethora of different resources made us entitle it

[9] *Shell Energy Scenarios to 2050.*

the sole energy-superpower, as long as none of the oil-rich Gulf states does not have it all, and with lots of reserves from each of the resources.

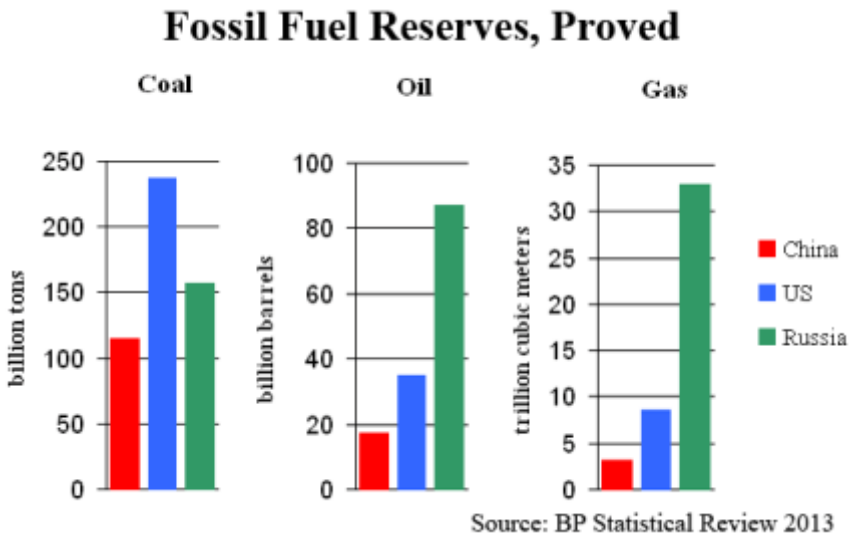


Figure no. 5. USA and China, the main consumers, versus Russia's reserves

Above mentioned discrepancy between the positions and interests of the USA and of China on one hand – in fact, latest their interests are almost identical - and the one of Russia might also suggest a different point of view on the recent developments in a number of countries.

3. Security threat: being on the oil route

If we understand the role of fossil fuels in today's security environment, we do have to remind ourselves where they can be found: not only the largest part of them, but also the best possible quality – which means the lowest degree of processing needed – and the easiest possible access – the joke of the Arab playing with his toe in the desert's sand and oil coming out of the drilling isn't any longer valid, but same time also not too far fetched – are in the Middle East. Even though oil and liquefied gas have to leave the area by some of the world's most dangerous choke points[10], there still is a water way to bring the precious goods out of the producer region in an almost safe way. Not same can be said about the second largest fossil fuel reservoir the world has: the close by Caucasian region of the '-stans'. This landlocked region has only following ways out: Afghanistan and Pakistan to the South; or the Black Sea countries to the East for Western consumers; the Moslem and independence seeking region of Xingjian in and for China.

If one overlaps the map of ongoing conflicts with the map of the fossil fuel reserves of the world, they do not match properly. But they match, if we add to the map of resources the one of the routes on which one could extract above mentioned resources and bring them to the consumer. Another match is even more striking: if we overlap the map of the conflicts with the map of resources and with the one of the religions of the world we will have another surprise: we will have another almost perfect match again, as long as 85% of the world's fossil fuels are on Moslem ground (and here we do count in also the Russian, Indonesian or Chinese territory) – and 60% of these Moslem hands do pray as the Shia are doing it.

[10] http://www.foreignpolicy.com/articles/2006/05/07/the_list_the_five_top_global_choke_points

Conclusions

The readers of geopolitical theory are familiar with terms such as pivot, containment, Realpolitik, but also names like Gladio do ring a bell. Some might even be aware of the role Lee Raymond, Exxon's CEO, played back in 2003 in the arrest of Mikhail Khodorkovsky's, after telling Wladimir Putin into his face that yes, once he entered as a stake holder in the former state-owned company Yukos, he will have the calls on the faith of its fossil fuels[11]. Or that Russia faces a flood of Chinese immigrants through its Chinese border and that this situation might create a demographical and political problem sooner or later[12] that would ironically remind some on the Crimean annexation. Even though it was published back in 1997, the theory of the extremely influential Zbigniew Brzezinski regarding the role of Turkey and Ukraine in the Black Sea region[13] cannot be forgotten by any of its readers. And it makes one think. Think about the US-Chinese run for oil in Sudan which led to the splitting of the country[14]. Think about the civil war Syria has to face after the gas discoveries and the way the now called terrorist movement ISIS[15] appeared, just as Hezbollah and the Taliban movement before, or the way not only Al Qaeda and the Chechens shared the same sponsors. Think about the coups d'etat Turkey had to face during the 20th century and the problems now president Erdogan has to face. Think about Romania's neighbour Ukraine and how close it is to the faith of a failed state. And how easy a failed state can be controlled.

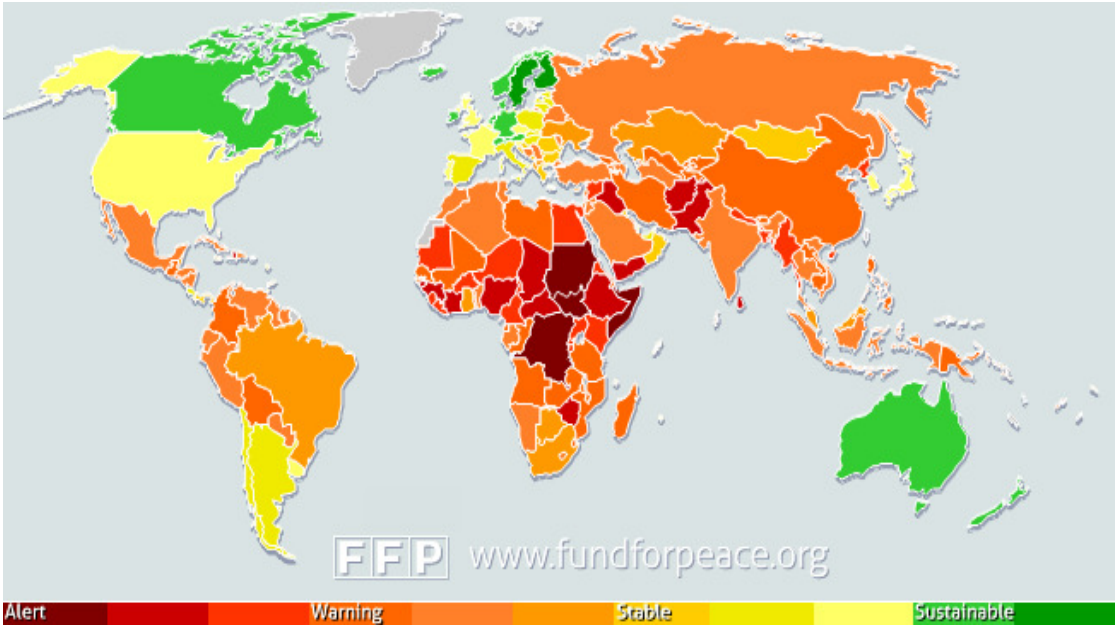


Figure no. 6. Failed states, brown meaning alert, orange –warning, yellow – stable, green - sustainable[16]

From the map of the failed states presented in figure 6 we can learn the Romania's yellow has also a strong orange shade in it. It will for sure depend also on the geopolitical and energy security knowledge of the president to be elected these days if the shade of yellow is

[11] http://www.commentarymagazine.com/2012/05/01/exxonmobil-role-in-khodorkovsky-arrest
[12] http://abcnews.go.com/International/story?id=82969.
[13] Zbigniew Brzezinski, *The Grand Chessboard*, Basic Books, **ISBN-10:** 0465027261
[14] http://csis.org/story/africa-china-united-states-and-oil.
[15]http://www.dailystar.com.lb/News/Middle-East/2014/Jul-26/265255-syria-regime-retakes-gas-field-from-isis.ashx.
[16] http://ffp.statesindex.org/rankings-2013-sortable.

going to darken or not over the next period of time. Because its geopolitical position – on the route out of the fossil fuels manhood is going to fiercely fight over in the next future – cannot be changed.

BIBLIOGRAPHY:

1. BRZEZINSKI, Zbigniew, *The Grand Chessboard*, Basic Books, ISBN-10**:** 0465027261.
2. ENGDAHL, F. William, *Mit der Öwaffe zur Weltmach – Der Weg zur neuen Weltordnung*, Rottenburg, Jochen Kopp Verlag, 2006.
3. KING, Hubbert M., *Nuclear Energy and the Fossil Fuels* http://www.hubbertpeak.com/hubbert/1956/1956.pdf.
4. MALTHUS, Thomas, *An Essay on the Principle of Population - An Essay on the Principle of Population, as it Affects the Future Improvement of Society with Remarks on the Speculations of Mr. Godwin, M. Condorcet, and Other Writers*, London, Printed for J. Johnson, in St. Paul's Church-Yard, 1798.
5. MEADOWS H. Donella, MEADOWS L.Dennis, RANDERS Jørgen, BEHRENS William W. III, The Limits of Growth ISBN 0-87663-918-X, 1974 second edition (paperback).
6. http://abcnews.go.com/International/story?id=82969.
7. BP Statistical Review of World Energy, 2011.
8. http://www.commentarymagazine.com/2012/05/01/exxonmobil-role-in-khodorkovsky-arrest.
9. http://www.cotidianul.ro/dupa-kosovo-consilierul-american-al-lui-ponta-e-interesat-de-minerit-in-romania-224772.
10. http://csis.org/story/africa-china-united-states-and-oil.
11. http://www.dailystar.com.lb/News/Middle-East/2014/Jul-26/265255-syria-regime-retakes-gas-field-from-isis.ashx.
12. http://ffp.statesindex.org/rankings-2013-sortable.
13. http://www.foreignpolicy.com/articles/2006/05/07/the_list_the_five_top_global_choke_points.
14. Group of authors:*Shell Energy Scenarios to 2050.*
15. Group of authors*: Russia's energy industry. Problems and prospects. – Moscow, Nauka, 2006,* http://russiancouncil.ru/en/inner/?id_4=588#top.
16. https://lh4.googleusercontent.com/-FHwzaPzQmSo/TYhT8klhZoI/AAAAAAAABlQ/xz8RkS-khOM/s1600/World-Population-and-Energy.gif, http://pictorial-guide-to-energy.blogspot.ro/p/list-of-charts.html.

PREVENTION AND RISK MANAGEMENT TECHNOLOGY IN THE SEVESO

Stelian-Ioan RECHIŢEAN
Colonel, PhD, Chief inspector at Inspectorate for Emergency Situations
"Tara Barsei" Braşov County, research field - prevention and management
of natural and technological risks.

Abstract: *In the third millennium the rhythm of change, as far as technology is concerned, is constantly growing, with obvious benefits. Usually, the negative effects of technological development are offset in time and space to the time and place the cause of action that generated. Awareness on the dangers of technology, effects on the environment and social implications have arisen as a result of serious accidents, which demonstrated the need for an integrated approach to the field. In the context of global concern problematic industrial accidents, preoccupations and actions in this area have existed since the 1980s, embodied in initiatives at global, European and national levels through the adoption of specific regulations on prevention, protection and response to emergencies caused by technological risks.*

Technological risk, as opposed to natural, can be controlled and reduced in several ways, but management requires more elaborate and customized for each category.

Keywords*: threats, disaster management, Seveso, obligations, prevention, intervention.*

Introduction

There is a real need for a rational and scientific discussion between all parties involved in risk management in Romania. Recent experience in emergency management in case of natural disasters and technological culture indicates a low level of security in the disaster.

Thus, it is necessary the develop activities which increase awareness of hazards in communities in the vicinity of industrial areas that show a high degree of risk.

Theme treats, the technological risk prevention and management in the context of the Seveso Directive is one of the topical areas of interest and date to achieve a co operational bases at local and national level, to implement policies to prevent major accidents, industrial and technological disaster management.

The paper deals with the implementation of the Seveso Directives: risk management, safety reports and policies to prevent major accidents and duties of operators, emergency communications, public information, making decisions, emergency plans.

1. Risk Management

Risks are a daily presence in the economy. Action harmful risk occurs both in economic loss, damage to facilities, equipment and the affected employees, the public and the environment.

The unprecedented development of the chemical industry has led to the production of the large quantities of toxic substances, many of which do not exist in nature. In the last century, the chemical industry has developed exponentially. This increase in the use and production of chemicals has led to the increasing number of accidents.

Keeping safe chemicals substances manufactured, which may explode, burn, asphyxiate, poison, corrode and generally affect people and the environment, it is not easy to do. This created the possibility that at any moment by accident (the disturbance, damage or deterioration of a machine or plant production, transport, storage and use) to be released into the environment very dangerous substances, usually toxic, so to occur a chemical accident. When released quantities and concentrations are high and effects on people and the environment are substantial, important and serious, can talk about the occurrence of disasters. These accidents have urged the promotion of European legislation to prevent and control this type of events, based on the principle "it is easier to prevent than to combat it."

Activity risk management developed both conceptually, and the practice became an industry in countries with functioning financial markets, but in Romania few organizations have developed their own mechanisms for measuring and hedging, others no do not know the benefits they would get by applying the procedures already established.

For several millennia, until the Industrial Revolution, the risks remained somewhat the same, known and identifiable by the community.

Technological disasters can be classified as follows[1]:

- by genesis : industrial major accident on traffic routes, accidental pollution, collapse (fall) cosmic objects, nuclear, mass fires, failure of public utilities.
- by scale effects : catastrophic, serious, minor or negligible.
- after propagation speed : fast, slow.
- after area affected : Global systemic, regional global, regional, local and punctual.
- after technological risk matrix.
  - category 1 - High risk - that action is required to prevent the incident or to minimize the consequences;
  - category 2 - Medium risk - will be analyzed to determine where cost-effective means of reducing risk;
  - category 3 - Low risk - which does not present a major accident hazard potential. Risks of category 1 are subject to a further assessment of consequences and likelihood (frequency).

Risk management is main stages[2]:

- Identifying hazards as a starting point for the risk assessment;
- Qualitative and quantitative risk analysis;
- Cost-benefit analysis related to change management and decision making.

Any risk analysis study primarily aims to establish acceptable limits.

In the studies of risk analysis are particularly important the following questions:

- The weakness may occur in the management of the security system that does not work;
- What are the preventive measures that can be taken to control the risk;
- How those actions are tracked;
- If the economic operator do things right, do things that have made its objectives and targets in the studies of risk analysis.

Risk indicators most commonly used are[3]:

- Dow index;
- Substances hazard index (SHI);
- Material hazard index (MHI);
- Chemical exposure index (CEI);

[1] Adriana BĂDILĂ (eds.), Disaster risk management, ALMA-RO, 2007.
[2] *Ibidem.*
[3] Şerbu Traiean, Risk Management-Elements of theory and computation, Publishing Ministry of the Interior, Bucharest, 2002.

- Index of fatal accidents (FAR);
- Index lost time due to injury (LTI);
- Rate the severity of lost time due to injury (LTIS);
- Frequency of accidents in transport and distribution;
- Frequency of absenteeism (ABS);
- Mond index (Crowl, 1990).

This requires reference benchmarks (indicators) used at different levels. It is obvious that we can not reduce risk to zero, therefore appears paramount limit value that can be supported by people in current activities.

Studies have established a risk acceptability curve. This curve allows differentiation between the acceptable and unacceptable risk. Thus, the risk of an event A, with serious consequences, but very low frequency, below theacceptability curve isconsidered acceptable and the risk event B, with less serious, but with a higher probability of occurrence of whose coordinates are above the curve, is unacceptable.

The likelihood of technological risk was determined by groups of intervals specified in IEC - 812/1985 and are:

- Extremely rare: p <7.10 h -1;
- Very rare: 7.10 <p <5.10 h -1;
- Rare: 10-5 <p <4.10 h -1;
- Uncommon: 4.10 <p <3.10 h -1;
- Common: 3.10 <p <2.10 h -1;
- Very common: p> 2.10 h -1.

For industrial installations severity (severity) is an important element for risk assessment technology. Therefore, corresponding to the seven grades of severity may be associated seven risk levels, in ascending order, and 7 levels of security (inversely proportional).

2. SEVESO Directives - history and actuality

Seveso is the name of a town in Italy, north of Milan, where, on July 10, 1976, a chemical accident occurred at the pesticide factory INCESA. The production of trichlorophenol by overheating has been eliminated in the form of extremely poisonous atmosphere tetrachlorodibenzodioxines. The accident caused the release of about 6 tons of toxic substances. This accident was a wake-up call that has led the European Community to take measures to prevent similar situations.

After the accident at Seveso, the European Community has defined a "major accident" (high risk) as an event (a substance emission, fire or powerful explosion) in relation to the uncontrolled development of technological activities that generate a serious danger inside or outside the company by issuing one or more toxic substances.

Directive "Seveso I" Council Directive no. 82/501/EC[4] on the major-accident hazards of certain industrial was adopted June – 1982, includes a set of bonds covering employees of industrial plants and national authorities. According to this, the European Commission is aimed at identifying and controlling major risk of major accidents at industrial plants.

Other accidents have occured over time.

- One of the most serious technological accidents occurred on December 3, 1984 in Bhopal (India) by accidentally dropping a toxic gas (methyl isocyanate) from a pesticide plant belonging to the International Union Carbide Corporation.

[4] O.J. No L 230 of 05.08.1982.

• In 1986, an agrochemical factory in Switzerland, attached to Basel, belonging to a powerful corporation Sandoz fire led to the pollution of the Rhine River due to leakage of 30 tonnes of chemicals (inks and fluorescent dyes, organophosphorus pesticides, a mercury-based fungicides). Basel city was hit by a cloud of mercaptans. It is estimated that 500,000 fish were killed, and the consequences of this accident were felt in the long term.

• The Piper Alpha, England on July 6, 1988, on the oil drilling platform there were an explosion and fire that killed 165 workers. There was an emanation of hydrocarbon condensate that reached into the air and exploded.

These accidents resulted in the amendment of Directive 82/501 / EEC (Seveso I). On December 9, 1996 Seveso II was adopted, following that dated February 3, 1999 to be applicable to the Seveso II Directive by EU Member States.

Directive "Seveso II" - Council Directive no. 96/82/EC[5] on the control of major accidents caused by hazardous substances emphasis on environmental protection and presents for the first time in the application materials that go as dangerous for the environment - particularly water.

The new Directive "Seveso II" aims to prevent serious accidents involving dangerous substances and limit their consequences to people and the environment, to ensure an effective default and a high level of safety within the community.

This directive includes the risk management aspects of the emergency plans and specifications imposed on operators.

Directive is transposed in Romania through Government Decision no. 95/2003 on the control of activities of major accident hazards involving dangerous substances.

A number of technological accidents with cross-border and international echoes have led to changes in the Seveso II Directive, taking into account other activities, including those related to mining.

On September 21, 2001, there was a very strong explosion at the AZF fertilizer factory (nitrate, France) in an industrial area near Toulouse, in southwestern France. The force of the explosion created a crater with a diameter of 50 meters and a depth greater than 10 meters. The blast broke windows from windows located in the city center 3 km away and the phone lines were down immediately, within a radius of 100 km.

On January 30, 2000 in SC Gold S. A. Baia Mare that has as activity recovery of gold and silver by treating tailings ponds at a pond where they were stored waste, a crack appeared and created a breach in the dam priming a length of about 25 m . This has led to the discharge of water suspensions and cyanide, cyanide contamination of rivers Lapus, Somes, Tisza and Danube rivers affecting the fauna and flora contaminated, contamination of about 20 ha of agricultural land, contamination of nine wells in the town Bozânta Mare.

Thus, the new *Directive "Seveso III" - Council Directive no. 2003/105/EC*[6] or Toulouse I appeared, modifying the scope of expansion in some sectors not included in the previous directive and also change the limits of some substances.

Seveso III Directive (2003/105/EC) was implemented in Romania by Government Decision no. 804/2007 and establishes two classes of risk (major and minor) for industrial facilities that use or store hazardous substances.

The aim of the Seveso III is, first of all,the prevention of major accidents involving dangerous substances and secondly limit the consequences both the health and safety of people and the environment. Its provisions apply to activities involving dangerous substances (toxic, very toxic, oxidising, explosive, flammable, highly flammable, highly flammable and dangerous for the environment).

[5] O.J. No L 10 din 10.01.1997.
[6] O.J. No L 345 din 31.12.2003.

Obligation to take all necessary measures to prevent major accidents and limit their consequences on human health and on the enviroment lies with both operators, holders of such activities and public authorities.

3. Implementation of the Seveso Directive in Romania

Competent authorities to implement the provisions of the Seveso Directive are[7]:

1. National level

- Ministry of Environment and Climate Change
- Secretariat of Risk;
- National Agency for Environmental Protection;
- National Environmental Guard.
- Ministry of Interior through the General Inspectorate for Emergency Situations

2. County level

- Inspectorate for Emergency Situations
- County Agency for Environmental Protection
- County Commissioner of the National Environmental Guard

In light of the Directive, operators, who are subject to its provisions, have the following obligations[8]:

- Preparation of a notification activity;
- Drafting a policy to prevent - a document that guarantees a high level of environmental protection and health;
- Writing a safety report - complex document on which the assessment is made on the site emergency management;
- Drafting an internal emergency plan that includes measures to be applied within the site;
- Testing and evaluating internal emergency plan;
- Review internal emergency plan in three years and safety report in five years;
- Notification of authorities in the event of a major accident;
- Notification of changes in structure, substance, quantity, organization;
- Public information on risk exposure, substances present, protection measures and behavior;
- Provide information for the authorities to external emergency plans.

Inspectorate for Emergency Situations in the context of the Seveso Directive has the following obligations[9]:

- Identification and inventory of operators subject to the provisions of HG. 804/2007;
- Check the major accident prevention policy and safety reports;
- Endorsement of internal plans;
- Develop external emergency plans;
- Review of external emergency plans;
- Organization system inspection and objectives identified (inspection planning, inspection reports, inspection reports synthesis);
- Territorial planning (safety distances between establishments covered by HG. 804/2007 and residential areas);

[7] Government Decision no. 804 of 25 July 2007 on the control of major accident hazards involving dangerous substances, published in the Official Gazette of Romania, Part I, nr.539 from 08.08.2007, article 5.

[8] Government Decision no. 804 of 25 July 2007 on the control of major accident hazards involving dangerous substances, published in the Official Gazette of Romania, Part I, nr.539 from 08.08.2007, article 7, 8.

[9] Government Decision no. 804 of 25 July 2007 on the control of major accident hazards involving dangerous substances, published in the Official Gazette of Romania, Part I, nr.539 from 08.08.2007.

- Prohibition of the use, operation and commissioning of sites where it is found serious deficiencies in the implementation of prevention of major accidents;

- Investigation of major accidents occurred objectives covered HG. 804/2007;

- Approval testing schedules internal plans;

- Planning external testing plans;

- Implementation of practical exercises to test external emergency plans.

For risk mitigation, Inspectorate for Emergency Situations with the Environmental Protection Agency Brasov and Brasov County Commissioner of the National Environmental Guard should take the following measures:

- To identify and inventory locations that are subject to the Seveso Directive;

- To provide specialized assistance for the preparation of continuously accurate notifications of substances on sites identified and their correct classification in the Directive, through the specialists responsible institutions;

- Analyze and validate safety reports and major accident prevention policies, prepared by external experts;

- Identify sites and groups of sites where there is potential risk of a major accident and its amplification by the effect of "Domino", due to location;

- To transmit local authorities information on the location of Seveso objectives and areas of emergency planning, in order to be considered in the development policies of the territory, so as to reduce risks to the population;

- Set up commissions to investigate major incidents Seveso sites products and conduct rigorous investigations of incidents that might occur;

- To organize a rigorous inspection and well planned on a systematic assessment of each site. Upon completion of inspections to end a joint inspection report. Subsequent to monitor the implementation of the measures imposed compliance.

The system aims inspection and planned and systematic examination of the systems used on site, whether technical, organizational or management so as to ensure that[10]:

a) the operator can demonstrate that it has taken appropriate action in relation to the different activities taking place on site in order to prevent major accidents;

b) the operator can prove that he used appropriate means to limit the effects of major accidents in and / or off-site;

c) the data and information contained in the safety report or other document filled adequately reflect site conditions;

d) Information was provided to the public.

In the same context, the Inspectorate for Emergency Situations conducts a series of activities which include:

- Have been inspected and approved internal emergency plans prepared by external experts;

- Have been developed external emergency plans and track the updating and revision based on changes made to safety reports and internal emergency plans.

Their purpose is planning a unitary measures necessary to protect life, property and environmental quality objectives outside sites in case of major accident involving dangerous substances.

External Emergency Plan aims to:

a) achieve in a short time, in an organized manner and in a unitary protective measures and actions, in case of a major accident;

b) reduce the impact on human health around the site on environmental quality and integrity of the property;

[10] Government Decision no. 804 of 25 July 2007 on the control of major accident hazards involving dangerous substances, published in the Official Gazette of Romania, Part I, nr. 539 from 08.08.2007 article 18.

c) informing and alerting the appropriate people;

d) planning arrangements for evacuation of the population at risk in emergency situations;

e) establishing procedures for the action off-site response forces.

- Have endorsed testing schedules internal plans and the inspections to verify their achievement;

- Planning the testing was performed external emergency plans. Exercise testing exercises were organized as complex multi-objective and intervention engagement of all parties.

Inspectorate for Emergency Situations is considering short and medium term projects to mitigate the risks and increase the safety of the population and environmental factors relating to:

- Conduct activities for startup in safe facilities;
- Securing sites on industrial sites;
- Monitoring activities in locations that are subject to the Directive and industrial parks in the immediate vicinity thereof;
- European funds by local governments for provision of technical and material intervention;
- Specialized training professional staff and voluntary formations specific risk management;
- Information and training measures for the population about the risks caused by traders Seveso and the behavior in case of accidents;
- Identifying new locations that are subject to the Directive and tracking compliance with the law.

To ensure improvement of prevention in the Inspectorate for Emergency Situations I think we need to focus on preparing Seveso inspections objectives, aiming to:

- Planned and systematic checking of technical systems, organizational and management specific objective of such
- Respecting the procedure for inspection and objectives Seveso
- Establish jointly with representatives of the County Commissioner of the National Environmental Guard inspection program
- Provision of modern equipment for emergency intervention (special vehicle research CBRN detector / portable gas / toxic substances)
- Provision of portable equipment for CBRN decontamination of personnel, equipment and special vehicles
- Identify new methods of preparation for emergency intervention to extend their knowledge on the objectives of the guards Seveso intervention (hazardous substances they work, their properties, safety data and method of intervention)
- Execution by intervention guards of training sessions in real conditions in which to be tested including intervention techniques and equipment.

Conclusions

From literature and specialized experience, I realize that often people's economic and social activities, and environmental components may be troubled by the tragic effects of natural phenomena (disasters) or human actions runaway (disaster) that can produce destructive and violent disorder of a system or predetermined situations.

Produced usually abruptly, by surprise, warning time being short (or in some cases absent, depending on the degree of economic development of the country in which the disaster occurs), the largest losses are recorded shortly after the event (number of victims

among people and animals, destruction of large volumes of goods and material values, ecological imbalance).Besides those listed above, calamities and disasters also cause serious mental and moral impaired population covered by this phenomenon. But extreme natural events are not considered hazards without causing human casualties and damage. A tornado or an earthquake occurred in a secluded, unpopulated place is an extreme natural event, but not a natural hazard. Natural hazards thus result from the conflict between geophysical process and people. This interpretation of natural hazards is that the central role belongs to people, not only through their location (hazards are only where people live), but also through the perception and their sizing.

On the other hand, what could be considered a minor incident in a developed country can be considered a major emergency disaster value in a country with opportunities for response (intervention) lower in such situations.

According to a report by the United Nations Centre for Emergency Assistance Environment, an emergency can turn into a crisis when there is something wrong in the activity response in such a situation. So, urgency, if not controlled, can easily escalate into a disaster due to exceeding the possibilities to cope.

If, in one way or another, the crisis may be directed, the disaster may be removed.

So, by using a specialized management of the crisis, its course can be changed.

Term response refers to any action that takes place when an emergency actually occurs and then, to reduce its negative effects on human health, economic and environmental activities.

Emergency response is a part of disaster management including prevention, preparedness, response and recovery. It is useful to distinguish four phases of response:

- assessments of the situation;
- stop to limit adverse effects;
- post-emergency assessment of environmental damage caused;
- rehabilitation of water, air and soil or other environmental elements affected.

The beginning of this millennium is characterized by a more pronounced impact of human activities on Earth, leading to global environmental changes, compounded by natural hazards. The magnitude and frequency of hazards linked more closely demonstrates the rapid growth of world population, especially in unfavorable regions, where extremes and imbalances occur increasingly sharper environment.

BIBLIOGRAPHY:

1. BĂDILĂ, Adriana (eds.), Disaster risk management, ALMA-RO, 2007
2. CARTAULT Jean Luc, Crisis Management, INESC-France Scientific Session, Sixth Edition, Fire Department, May 2003
3. POPA I and EPURE M LAURA , Disaster Management, Company INEDIT SRL, Bucharest, July 2001
4. POPESCU DORIN and PAVEL ALECSANDRU, technical risk / technology Brilliant Publishing, Bucharest, 1998
5. SERBU, Traiean, Risk Management - Elements of theory and computation, Publishing Ministry of the Interior, Bucharest, 2002
6. STAINER, Nicolae; ANDRICIUC, Radu Fundamentals of crisis management and civil emergency civil protection perspective, Ed. Edit Consult, Bucharest 2004
7. Council Directive no. 82/501/EC of 24 June 1982 on the major-accident hazards of certain activities industries - "Seveso I", OJ No L 230 of 05.08.1982
8. Council Directive no. 96/82/EC of 9 December 1996 on the control of major accident hazards involving dangerous substances - "Seveso II", OJ No L 10 of 10.1.1997

9. Council Directive no. 2003/105/EC of 16 December 2003 amending Directive Council of Europe no. 96/82/EC - "Seveso III" O.J. No L 345 of 31.12.2003
10. Commission Decision 98/433 / EC on harmonized criteria for dispensations according to Article 9 of Directive 96/82 / EC, OJ No L 192/1998
11. H. G. No. 804 of 25 July 2007 on the control of major accident hazards involving dangerous substances, published in the Official Gazette of Romania, Part I, 539 of 08.08.2007
12. *** An Overview of Disaster Management – 2nd Edition -, UNDP, ONU, 1992

ISO STANDARDS APPLICABLE TO INTERNAL AFFAIRS DOMAIN IN THE FIELD OF RISK MANAGEMENT

Georgică PANFIL
Chief inspector, PhD lecturer within "Alexandru Ioan Cuza" Police Academy.
E-mail address: panfil.george@gmail.com.

Abstract : *The article tackles the area of Internal Affairs and is dedicated mainly to the international standards provided by International Organization for Standardization and their compatibility with risk management activities in this domain. Furthermore, the author presents his own conclusions linked to the necessity of standardization of the domain of Internal Affairs.*

Keywords: *standardization, ISO, Internal Affairs, risk management.*

1. General concepts related to risk management

In every type of organization daily tasks are fulfilled or not depending of different causes. In order to have efficiency, it is an obvious necessity to have implemented a good program of management from the decision factors. Within any management workflow, one must take in consideration different issues and different factors that could interact with the organization itself. The manager of a certain institution should not limit himself to treat or solve the consequences of an event already produced. Treating the consequences never solves the problem of the causes that have initiated the event at its origins, and thus there is a probability to have the negative event repeated sometimes into the future. What once happened has the potential to come again, usually with an increased frequency and a superior negative impact on the organization and its objectives. This is the reason why when one would tackle the concepts of management, he should also refer to problems linked to the idea of risks and risk management.

The first problem to be approached is linked to the concepts defining *risk* and *risk management*. Currently there are many definitions of the term of risk, with aspects of specificity related to the area of reference of different authors. In some opinions, risk means "a future problem that can be avoided or diminished", while in other approaches risks are "elements to be immediately dealt with". In accordance with the definition provided by International Standardization Organization (referring to the area of information security), risk means "the potential of a given threat to exploit the vulnerabilities of a structure or organization in order to endanger the objectives of that institution". It is also appropriate to refer to the opinion emitted by Ulrich Bech, providing a social approach of the term of risk. As follows, within modern society, providing welfare is done only in relation of a systematically emission of risk. As follows, individuals have the tendency to identify vulnerabilities of modern world and if possible to exploit them. As such, risk can be considered to be a systematically way of management of the insecurities induced by social development itself. Beck also states different categories of risks, such as physical ones (capable to destroy life, like radioactivity, toxic residues, wars), but also social and cultural risks (linked to education, evolution of crimes etc.).

On the other hand, referring exclusively to basic dictionaries, a more simple approach would define "risk" as "safe".

From the analysis of different opinions related to risks, the main conclusion is that risk itself is a complex term based on three variables:

- probability of a *threat.* A threat represents the probability of an action, inaction or phenomenon to generate losses to a person or to an organization. Most often, threats come from the outside an organization, but it may as we'll come from the inside. For example, in relation with the system of Internal Affairs, a threat can be considered an insider providing sensitive intelligence from the classified files of Romanian Police.

- probability of an exploitable *vulnerability***.** The vulnerabilities are states of fact, processes or phenomenon linked to internal environment of an institution, able to diminish the capacity of reaction to a risk, or at least able to favor the apparition or development of a risk. Romanian dictionaries define threat as the attribute of a system to be easily attacked, to have sensitive areas[1]. The main characteristic of a vulnerability is that it comes from the inside, while a threat will usually come from the outside. In relation with the previous example with the mole, the vulnerability is the inefficiency of the system (police) to prevent and identify in proper time the leak of information.

- a potential *impact* on the organization. Oxford Dictionary[2] defines the impact as "a marked effect or influence". Should we extend the definition in relation with our needs, the impact represents the damage taken by the organization in care of risk materialization. The idea of risk exposure refers to the consequences related to pre-established objectives, in case of risk materializations, as a combination of probability and impact[3].

Referring to the previous example, risk is provided by the possibility of an intelligence leak, offering the potential to endanger the safety of police workers, the objectives of police itself and ultimately the legitimate interests of the state.

Risk management refers to all processes and procedures developed and all the measures taken by the manager (or Management Authority, if case), in order to identify risks, vulnerabilities and threats, to evaluate and characterize them, as well as taking the appropriate measures to minimize them, revision the process and continuous monitoring. It has to be said that at the bottom of risk management process is the concept of risk analysis, meaning tackling, analysis, identification, quantification and characterization of a given risk.

2. Risk management and Internal Affairs

In the area of Internal Affairs, threats and the possibility of their materializations are common problems. However, these types of threats do not reside only in one domain (economy, commerce, politics etc.), but can have their origins in so many sources, that we might be tempted to state that threats may come from everywhere. Also, the very nature of the vulnerabilities within this area makes them almost impossible to accept, thus they must be faced immediately. In the field of impact and result of risk effects, the situation tends to be more than serious.

Currently there is a stringent need for tacking the domain of risk management, especially in the field of Internal Affairs. We must never forget the sensitivity of this domain and its place and role within the society. While a materialized risk in a private company is able to provide effect on local level, and only sometimes in the exterior, threats linked to law enforcement agencies and structures are definitely more serious and must benefit of an appropriate response. Referring to the example of sensitive intelligence leak, the impact can

[1] www.dex-online.ro, accessed on 5th of September 2014.
[2] http://www.oxforddictionaries.com/definition/english/impact, accessed on 5th of September 2014.
[3] PANFIL, Georgicã; General theories related to risk management, published in First volume of Proceedings of scientific studies, Estfalia Publishing, Bucharest, 2011, p. 175.

be of a limited scale (although limited is not a synonym to small in this case, as endangering the life o a person is a very delicate situation) of a medium scale or even a a large magnitude, providing blockages of the activity of entire sectors of police work. Let us imagine, in this case, the eventuality of a leakage of the list with all undercover agents fighting drug trafficking.

Within the area of Internal Affairs, the management process itself tends to be a challenge due to the specific of the structures involved. In some cases, the chief of the unit is the risk manager, while in other cases these tasks are fulfilled by other personnel. Beyond this, it must be remember the fact that all institutions from the area of Internal Affairs must face some constraints linked to decision all processes and sometimes to financial limitations.

At present, in the area of Internal Affairs, there are no types of dedicated courses of risk management. Of course, there can be found different types of courses (master courses, postdoctoral courses), but these are only at a general level and not focused on issues related to risks. Some of the current managers have followed their own studies in the field of risks, but these tackle only general concepts. As follows, the need of a unitary form of training for all the managers from this area tends to

3. The necessity of Standardization in Internal Affairs

Currently we face a general tendency - to be found in almost every domain - to acceding to the idea of "standardization". This concept is often subject to a wrong perception. Basically, the term defines the process to establish and apply a standard. Furthermore, a standard means either a level of quality or attainment, or something that is acceptable or desirable[4]. The main purpose of the idea of standardization might refer directly to recognizing and implementing some similar rules, procedures, principles, approaches etc., no matter the area of appliance, country, institution type etc., in order to guarantee that the organization to have implemented the standards (rules) are following similar workflows.

For a complete understanding of the concept of standardization, it has to be said that this term is included in more complex area, the one defining quality management. Quality management has a number of three components: accreditation (to have a reconnaissance from an official organization linked to the system of quality implemented), certification (to confirm the level of trust of a certain individual in a certain domain) and standardization (previously defined). To conclude, accreditation refers to an institution, certification only refers to individuals and standardization is usually linked to working procedures. All of those have a final objective - to prove quality. Of course, one could state that a certain institution provides quality work, but there is a certain necessity to both having *a trusted model* (a minimal set of conditions) to follow - that would be the standard, and furthermore *a special couple of bodies*, one to create the standard, another to evaluate the compliance with the standard.

It has to be said that most of the standards are provided by International Standards Organization, which usually creates a standard in a certain domain on request of a specific organization. However, usually standards are applicable to different organisms. Every country has (at least) one accreditation organism, an entity with purpose to ascertain the level of quality, the conformity and as follows the possibility of accreditation.

As previously stated, within Romanian Ministry of Internal Affairs the idea of quality has recently increased. Most of the bodies subordinated to this ministry have manifested preoccupation to implement different standards (usually general standards) in order to be accredited by Romanian Accreditation Body - RENAR. RENAR presents to every institution

[4] http://www.merriam-webster.com/dictionary/standard, accessed on 7th of September 2014.

a minimal set of prerequisites in order to be able to become subject of an evaluation. If an institution proves that it meets those minimal requirements, RENAR provides the reconnaissance of the institution's compatibility with that certain standard. At current level, within Ministry of Internal Affairs there is no unitary preoccupation to implement a certain standard. Each and every subordinated structure has implemented standards according to the decision of its director. Of course, there is a rational thing to have implemented a standard related to every structure's line of work (for example, in the area of forensic science, National Institute of Forensic Science has implemented standards related to laboratory analysis and crime scene investigation), but the main issue is that at current level there has not been established a minimal level of quality in all of those bodies. There are general aspects of the management process and related to quality assurance that should be followed in every institution. It is a fact that risk management and risk assessment are managerial methods used everywhere, yet we cannot say there is a common practice to have implemented dedicated standards linked to this area. Beside, budget constraints often have a role in this so-called chaos, due to the fact that most of the time the financial resources are barely enough to support the basic processes of the structures, thus the idea of allotting money for accreditation procedures cannot be out in practice. From our point of view, this could be easily solved if a certain percentage of the ministry's budget would be reserved exclusively to the area of quality assurance, not to say the idea of creating a strategy dedicated to the implementation of certain standards in every institution from the ministry's subordination. Nevertheless, we consider there is a great need for the education of the decision factors in order to recognize and, most important, understand, the necessity of standards implementation, especially in the area of risk management.

4. International standards used in the area of risk management with appliance in the domain of Internal Affairs

A standard is defined by Merriam Webster Dictionary as something set up and established by authority as a rule for the measure of quantity, weight, extent, value, or quality[5]. As we've stated before, the standards have general appliance and theoretically can be applied to any institution. At current level, we can discuss about general standards (with general directions and principles), and dedicated ones (for example with direct references to the domain of Risk management). For example, a general standard is ISO 9000, while standards like the ones included in the so-called "31000 family" are from the category dedicated to risk management. On the other hand, we can separate the standards provided by ISO (International Organization for Standardization) or IEC (International Electrotechnical Commission) - those being the most important bodies in the field of standards, and other bodies, such as British Standards Institute, New Zealand Standards, Institute of Risk Management etc. However, in direct compliance with the domain covered by our subject, this paper will only tackle the ISO standards.

As follows, the main standards to be linked to the area of risk management are: ISO 9001:2008, ISO 31000:2009/ISO 31010:2009 and ISO 73:2009.

Referring to ISO 9001:2008 - Quality Management Systems (QMS), it has to be said that is part of a larger group of standards[6] dedicated to the field of quality management from a general point of view (thus, this group integrates ISO 9000:2005, meant to approach basic concepts and principles in the area, ISO 9004:2009, linked to the efficiency of QMS, and ISO 19011:2011, related to the audits of QMS). This standard is actually one of the most frequent

[5] www.merriam-webster.com, accessed on 11th of September 2014.
[6] www.iso.org/ISO/iso_9000, accessed on 10th of September 2014.

implemented standards worldwide, due to its general management principles and it's compatibility with almost environment and organization. It is the only standard from the 9000 family that can be accredited, some of the structures from Ministry of Internal Affairs having it already implemented. The idea of being a general standard (concentrated merely on focusing on the final beneficiary and on the plus provided by the interest of top management in the context of constant improvements of the management processes), however, has its minuses, as within the general principles of this objective-based standard there cannot be found the process itself of risk management, thus the necessity to tackle another family of standards, that is the 31000s. However, a new revision of the 9001 standard is to issued in 2015, providing promises to include basic issue linked to risk management.

Referring to ISO 31000:2009 - Risk management, principles and guidelines we have to tackle it in consonance with ISO/IEC 73:2009 - Risk management vocabulary, as they both refer tot the same domain, one providing the connects, definitions and generic terms, the other the basic framework of the risk management. Plus, one should also focus on a related standard, ISO 31010:2009, concentrated on risk assessment techniques and fundamental concepts, due to the fact that risk assessment is a vital component of the risk management.

Within the vision of ISO 31000, risk management processes should be adapted to the realities and the organization specific, integrated within the general management workflow and also embedded in the culture and practices of the organization[7]. Beyond the introduction layer of this standard, tackling the terms, definitions and principles (sashes linked to manager's mandate and commitment, knowing the organization, establishing risk management general policy, accountability etc.), the most important part of it is concentrated to the risk management process and framework. Within the vision of ISO 31000, first step to be followed in order to integrate an efficient policy of risk management is creating an appropriate context within the organization and defining risk criteria (levels of acceptance, defining the purpose of risk management, establishing responsibilities, identifying the resources, defining risk assessment methodologies to be used etc.). Risk criteria refers to the acceptable level of risk for organization, time frames for reactions, the way to determine risk, measuring the consequences etc.

The standard considers the risk management process to be composed from the following steps: risk identification[8], analysis[9] and evaluation[10] (these three activities are known as risk assessment) and risk treatment (taking options like accepting the risk outcome, eliminating the risk source, minimizing the threat's occurrence etc.). In parallel, there are constant workflows in the area of communication/consultation and monitoring/review. Furthermore, the entire process is recorded thru specific methods.

At current level, ISO 31000 cannot be used for accreditation. However, individuals can obtain certification in this domain - many courses and training programs based on the 31000/31010 standards. For personnel placed in management positions it should be a must to attend this form of training. From the point of view of the 31010 standard[11], which contains an explained approach of the risk assessment process (risk analysis - tackling the way to describe the consequences, estimation of probability, analysis of likelihood etc., risk

[7] ISO/FDIS 31000:2009, p.13.

[8] Identifying the risk means establishing the sources of threats and vulnerabilities associated, and provides basis for further analysis in next step. It is very important not to neglect any possible source, as in next steps only the identified risks are analyzed.

[9] Risk analysis deals with understanding the risk, the positive and negative impact on the organization, and furthermore the probability of occurrence.

[10] The part of risk evaluation compares the analyzed& explained risk with the risk criteria previously established and provides the basis for risk treatment measures.

[11] ISO 31010:20009.

evaluation and the monitoring phase) and especially of the main risk assessment techniques, we should observe that is not only intended for training the manager, but also those members of the organization in charge with the analysis of the possible events. Should there not be such a person within the structures from Ministry of Internal Affairs, we consider there is a necessity to assign and most important train one, as some tasks cannot be carried out exclusively by the manager - in this case, he is supposed to take decision based on the assessment provided by such a specialist.

Personal conclusions

To imagine our current society without rules to follow is basically impossible. The rules are made to be followed by both citizens and public institutions. For a ministry of such an importance as the Ministry of Internal Affairs, one of the main conditions to exist and have proper operations is to be trusted by the society. For any public entity, who needs trust must provide quality. As such, quality assurance is a must for the ministry itself, and of course for all it's subordinated bodies. As we stated above, the components of quality come from human resource (thru certification of skills and aptitudes), from the workflows themselves and the procedures concerning them (thru aligning them with a defined standard) and from the aggregate processes evaluated and recognized by an external auditor (thru certification). The specificity and the complexity of the domain of Internal Affairs makes this a sum of domains, each with it own dedicated workflows. Workflows that, as we said, need to provide quality results. Beyond the necessity to align most of the domains with good-practice and international standards, there are some common things that need to be taken care of. The managerial process, with its specificity, is to be found in every structure. As such, in every structure there are to be found external and internal challenges - either weaknesses of the system, known as vulnerabilities, either potential dangers from exterior, known as threats. Some threats have a specific possibility of occurrence and to generate a damage to the organization, thus providing a risk to happen. It is in every manager's preoccupation to ensure the best parameters for its organization to function, dealing with the risk within risk management processes.

As stated above, some of the standards provide the possibility to accreditation of an institution - in the case of 9001 standards, it is widely implemented and recognized by RENAR within the structures of the Ministry of Internal Affairs, while other standards, like 31000 family are only meant to provide instructions - but, even without the possibility of accreditation, they provide also the fundamentals for certification of the individuals - in our case the managers in the field of risk management. Actually, we consider the 31000 family of risk management standards the best source for a real understanding of the risk management process in its vast complexity. We also consider a real necessity the existence of a document to provide the steps and the way of adapting the ISO standards to the necessities of internal affairs specificity.

BIBLIOGRAPHY:

1. PANFIL, Georgicã; General theories related to risk management, published in First volume of Proceedings of scientific studies, Estfalia Publishing, Bucharest, 2011.
2. PANFIL, Georgicã; Risk management associated to informational security, Estfalia Publishing, Bucharest, 2013.
3. ISO Standards Collection, electronic version.
4. www.dexonline.ro
5. www.oxforddictionary.com
6. www.merriam-webster.com

VULNERABILITY OF CRITICAL INFRASTRUCTURES AND RESILIENCE OF HUMAN COMMUNITIES TO NATURAL DISASTERS

Cristian HOCIUNG
Colonel, PhD, "Bucovina" Inspectorate for Emergency Situations, Suceava county, Romania.
E-mail address: hociungcristian@yahoo.com

Tudor HOCIUNG
MA student within National School of Political and Administartive Studies (SNSPA)
Bucharest, Romania.
E-mail address: hociung.tudor@gmail.com

Abstract: *Infrastructures, in an extremely summarized definition, constitute the reinforcement of every socio-economic system by which it individualizes, interacts with other similar systems, reaches a steady state and tends to work in they address.*

The economic development of the countries, varied both inside the limits of the same continent and at global scale, is reflected in the number, destination, density and territorial distribution of the national critical infrastructures.

Wars, terrorist acts, accidents of all kinds and mainly extreme natural phenomena are inducing outage and malfunctions of the national infrastructures, revealing their criticality.

At world level, there crystallized two trends in grounding the strategies of protecting the national critical infrastructures. The United States` option is based on increasing the state and federal response to hazards occurance. The EU countries agreed to adopt proactive measures – inside a joint subsidiarity, and integrated strategies, in order to achieve a sum of inter-operational reaction capabilities.

Key words: *infrastructure, criticality, communities, destructive, resilience, vulnerability, protection.*

Introduction

Every nation acts permanently to identify those essential infrastructures they owe and without which the whole society would suffer, as well as the specific factors which could endanger them.

The criticality of infrastructures is conditioned by their status of uniqueness within a system, "by the vital character as a material or virtual support in functioning of economic, political, social, military, informational processes etc. and by its irreplaceable role in the stability, reliability, functioning and security of the systems, vulnerabilities to direct risks and to those targeting systems to which they belong"[1].

1. Critical infrastructures - Evolution of the Concept

The concept of "critical infrastructure" was initially used after the Cuban Missile Crisis (1962), an extreme situation involving the USA and the Soviet Union.

[1] Filofteia Repez, *Protecţia infrastructurilor critice,* UNAP/CSSAS, 2012.

Among various other events of political, military and diplomatic origins preceding the crisis, from the very beginnings of the events the American president J.F. Kennedy and the Russian prime minister N.S. Khrushchev faced difficulties in communicating in real time. In order to avoid other tense situations, after easing the crises, there was made a direct and safe connection between the White House and Kremlin - the famous "red thread" - and the telecommunications became the first national critical infrastructure of the USA.

Following the bombings of the World Trade Center (1993) and Oklahoma City (1995) the phrase "critical Infrastructure" was officially used for the first time in analyzing the terrorist phenomenon on July, 15, 1996, in the text of the Executive Order No. 13010 for the Protection of Critical Infrastructures, a document signed by the US president Bill Clinton. Critical infrastructure is defined as a *"part of the national infrastructure which is so vital that its destroying or incapacity of functioning may diminish dramatically the defense or economy of the USA"* and included telecommunications, the system of electricity and water supply, the gas and oil deposits, finance and banks, emergency services (medical, police, fire brigade), as well as the government continuing.

Presidential Commission on Critical Infrastructure Protection, established in 1995, reached the conclusion that *"security, economy and survival of the industrialized world depend on three interconnected elements: electric power, communications and computers"*[2].

The terrorist risks multiplied in the years that followed on vital state objectives and facilities, but also at the headquarters of international bodies, simultaneously with their increasing number and importance. The terrorist acts of September, 11, 2001 at the World Trade Centre proved that one single country, no matter how powerful it is, can not provide by itself protection to all its vital elements.

The phenomenon of globalization, besides advantages and positive transformations, "creates serious breaches to fast propagation of direct threat to the security of all states". In order to minimize the vulnerability of the national vital objectives within the main governmental services and "to ensure the continuity of the political and economic life at any outage and to protect the population", In October 2001 the White House administration released a new *Executive Order for the Protection of Critical Infrastructures*.

The issues of defining critical infrastructures caught subsequently the attention of international bodies.

In NATO's acceptance, the member states consider the critical infrastructure as being "facilities, services and informational systems which are so vital to the nations that their outage or destroying might generate the destabilization of national security, national economy, health of the population and the efficient functioning of the government"[3].

Senior Civil Emergency Planning Committee inside the NATO appointed the subordinate committees to find the solutions to a unitary approach of the problems regarding the criteria for determining the critical infrastructures, the methods of analyzing the risk and determining the vulnerabilities, as well as the methods of protection. The NATO activities in the area of critical infrastructures in 2003 are part of a larger frame including also the Civil Emergency Planning - a concept document targeting the protection of critical infrastructure and Action Plan - addressed to the developing of the national instruments of managing the sequels of chemical, biological, radiological and nuclear incidents/attacks, as well as the consequences of natural disasters on critical infrastructures.

In Europe, the interest to clarify, by legislation, the elements reflecting the concept of critical infrastructure was also accelerated by the terrorist acts. The basic issues of the European security strategy were promoted at Paris, in March 2003, during the first

---

[2] Grigore Alexandrescu, Gheorghe Văduva, *Infrastructuri critice. Pericole şi ameninţări la adresa acestora*, UNAp/CSSAS, 2006, p.10.

[3] NATO - Senior Civil Emergency Planning, Prague Summit, November 2002.

multilateral meeting of G8 on protecting the critical infrastructures. After the terrorist attacks in Madrid, 2004, and London, 2005, the EU countries started actions of coordinating the policies in this area by initiating, in 2006, The European Program of Critical Infrastructure Protection. Directive 2008/114/EC imposed two sectors (services) of European critical infrastructures: *The Energetic Sector* (electricity - infrastructures and installations for producing and transporting; petrol - production, refining, treatment, storage and distribution via pipes and GNL terminals) and *Transports* - on road, railway, air, inland waterways, sea and ocean transport on short distances and harbours.

Besides the efforts of the EU countries' governments, there added those of the private sector, directly interested in protecting their own infrastructures, as well as of the NGOs and of the scientific community. The convergence factor of these processes was the tendency of the terrorist organizations to attacking mainly elements of physical and virtual elements of infrastructures. An example of the virtual critical infrastructures vulnerability is the attack on Estonia's cybernetic system, in April 2007. The system was blocked for over 60 minutes because of receiving some thousands of megabytes information packages from a hacker who couldn't be identified and neutralized at that moment. The fast collapsing of the whole cybernetic infrastructure of the country generated cascade effects on various other infrastructure elements. This event is considered to be the first ever cybernetic attack in history on a national state. Specialists say it was the most significant crisis of this type, both from the perspective of the non-conventional character of the threat which generated it and of its magnitude. Georgia was also the target of a methodical cybernetic attack only a few weeks before the outbreak of the conflict with Russia, in August, 2008.

The concept of "critical infrastructure" evolved on the background of identifying new elements of criticality of the infrastructures, increasingly diversified and depending on one another.

From the point of view of the strategy of protecting the critical infrastructures, it seems that the USA option is based mainly on the increasing of the capabilities of reacting to the manifestation of hazards.

European countries agreed to adopt mainly proactive measures, developing elements of subsidiary in an integrated European strategy and generating some productive and inter-operational reaction capabilities.

2. General Conditioning in Producing of Extreme Natural Phenomena

Everyday reality accustomed us to the manifestation of extreme natural phenomena with disastrous effect upon human communities and environment. The fast dynamic of the effects of global warming, along with the uncontrolled influence of anthropogenic factors are producing major perturbations to the natural balance of the Earth.

Statistics released after World War II revealed that the number of victims and the amount of damages after events of geophysical origin are exceeding those resulting from military actions and terrorist acts.

In this paradigm there is the justifying of an analysis of maximum generalization regarding the vulnerability of communities and implicitly of their critical infrastructures in the context of the more and more frequent manifestations of the extreme natural phenomena generating disasters.

Although the mapping of all the risky regions on Earth cannot be done with certain accuracy, the repeatability of some destructive events - scientifically demonstrated or statistically confirmed - yet reveals a clear and productive image of the threatened terrestrial surfaces. These surfaces circumscribe entities (countries or communities) with political and administrative organizing of their own and which possess natural resources, develop

economic activities, produce goods, services, facilities and infrastructures. Every nation is functioning as a system, has an organizational culture, specific interests and objectives.

In the relationship between human communities and extreme natural phenomena, it is necessary to make a clear distinction between *risk* - seen as being tolerable regarding the amount of damages, and *disaster/catastrophe*- generating serious malfunctions at society level, with losses that cannot be surmounted by the own effort of the affected country.

The sudden manifestation, with intensity and on large surfaces, of the natural risks and hazards is generating vulnerability to communities and countries, regardless of their level of organization or the economic development. In many situations, the effects of extreme natural phenomena have regional or even global impact (earthquakes, tidal waves, volcano eruptions etc.).

In general, specialists agree on the main conditionings which potentiate the producing of extreme natural events: global climate changes with local and regional impact; galloping industrialization; massive deforesting at world scale; uncontrolled expansion of the cities; civil constructions, works of engineering art, networks with varied destinations, other facilities are not safe to exploit any longer and loss of slopes stability.

The climate changes generate anomalies in general air circulation. Seasonal weather phenomena (tropical cyclones, monsoons, rainfalls) turned excessive and have offset manifestations in time, both on latitude and on altitude natural setting.

The global warming determines firstly the melting of the icecap and of the mountain glaciers, with incalculable effects upon mankind. What consequences will it have on the temperature and salinity of the ocean mass of water? How will it change the circulation of ocean currents and what impact will it have on the climate? Which will be the impact of the increasing water level of the oceans upon the coast areas in the following years (landscape, environment, communities and infrastructures)? Scientists have to deliver answers and global solutions to all these questions and the governments to act firmly in order to reduce the risks and preserve the environment.

Industrial development at global scale, besides major benefits in economic and social evolution of the contemporary society, produces deep wounds to the environmental factors. The population's needs - much larger at the beginning of the third Millennium - are more and more difficult to satisfy. Lester R. Brown warned in the nineties: "if ecosystems on which mankind depends keep on deteriorating, global economy can not expand any more without limits"[4].

Deforestation on large areas in order to extend agriculture, to exploit and capitalize the wood or to construct economic objectives (roads, dams etc.) has extremely serious consequences. The real dimensions of the massive deforestation is revealed mainly by the diminished volume of oxygen produced and delivered in the atmosphere. The sickness of the soil left after deforestation decreases rapidly, its capacity of water retention from the rain decreasing as well. The decrease of afforested surfaces obliges the wild animals - potential various diseases carriers - to leave their natural habitat and migrate to inhabited areas where, in contact with humans, may transmit diseases which can generate epidemics hard to fight against.

The uncontrolled expanding of settlements generated occupying improper territories with high geological, geomorphological or hydrological risk level. Settlements and infrastructures built along the major riverbeds are permanently exposed to floods. There can be mentioned countries of the Southeast Asia (Pakistan, China, India, Bangladesh) but also from South America and even Europe. At the same time, settlements on slopes are threatened

[4] Lester R. Brown, *Starea lumii*, Editura Tehnică, 1999, p. 32.

by floods generated by hard rains. Human habitats developed on earthquake risk areas are extremely vulnerable to seismic moves and, depending on the ocean proximity, to tidal waves.

By the diminishing of the structural resistance and safety in exploitation, constructions and infrastructures may generate themselves disasters: floods, fire, explosions, contamination of the population, animals and environment. We speak about dams, bridges, viaducts, tunnels, chemical works, nuclear power stations, hydro power stations etc.

3. Risks of Extreme Natural Phenomena on Critical Infrastructures

The declared target of this paper - a general argumentation of the consequences of extreme manifestations of natural phenomena on communities - requires a particular approach of the main risks associated with critical infrastructures.

Extreme natural phenomena which manifest at global scale or on large areas are: reversal of the Earth's magnetic poles; falling of cosmic bodies; hard earthquakes; volcano eruptions; hurricanes; solar storms; landslides (involving the loss of stability of dump tailing dams); prolonged drought; heat waves; massive snowfalls, snowstorms and extremely low temperatures.

Reversal of the Earth's magnetic poles is a rather improvable event for the predictable future. Although the mechanism of this geological phenomenon is not known exactly, some scientists consider that "it is generated by the convective moves of the liquid iron in the external core of the Earth[5]". This theory is also supported by Professor Peter Olson from the Harvard University, who considers that the phenomenon is inevitable because "the Earth's magnetic field is the result of the process of friction between the layers of its nucleus"[6].

The concept was imposed on public, somehow speculatively, by promoting the phenomenon as imminent, in the context of the weakening of the Earth's magnetic field power. The planet's magnetic field acts like a shield protecting the atmosphere against solar wind. During a reversal of geomagnetic polarity the magnetic field decreases dramatically and exposes the atmosphere to the entire solar flow/wind, which determines the release of oxygen ions in space. The effect is the triggering of mass extinctions by wasting the atmospheric oxygen, as results of the researchers of the Chinese Academy of Science say. Independent studies demonstrate that the loss may reach 9%.

Real consequences on mankind can be catastrophic. How would living organisms react to such a change? Or, more specific, what effect could the phenomenon have on blood flow or on plant sap circuit? Could the value of terrestrial gravity modify? Would the effects be permanent or only temporary?

Falling of cosmic bodies/fragments (meteorites, asteroids, comets etc.) are phenomena of daily manifestations; estimated 100 tons of meteorite material are falling on Earth daily, most of it under the shape of particles. The falling of some meteorite fragments, on February, 15, 2013, in the Chelyabinsk area (Russia) proved total vulnerability of the society to this type of hazard. The meteorite, with a diameter of about 15 meters and an estimated weight of about 7.000 – 10.000 tons, disintegrated because of the overheating and melted in contact with terrestrial atmosphere. Incandescent fragments fell in the above mentioned area affecting 7 settlements. The danger on infrastructures, on communities is generally measured according to the size of the fragments and the place of impact with the terrestrial surface. If meteorite fragments had fallen over much more populated urban areas, the number of the victims and the volume of damages would have been many times higher.

---

[5] *Nucleul Terrei se deplasează brusc*, 23.06.2008, http://www.descopera.ro/dnews/2733343-nucleul-terrei-se-deplaseaza-brusc, accesat 03.09.2014.

[6] Peter Olson, *Efectele mantalei interioare asupra geodinamismului*, 2003.

Earthquakes represent the most destructive natural events. The unpredictable earthy movement, violent and of a very high intensity, produces a multitude of serious consequences on a region. Definitely, the number of victims is the most important and tragic criteria of evaluating their effects. Practically, consequences of an earthquake sum up all categories of damages produced by the other hazards (flood, landslide, fire, technological accidents), but at considerably higher dimensions, in terms of quantity and value. After such a major event, the vital systems of society may get disorganized.

We consider it necessary to remind some essential discriminatory elements of the consequences of some major earthquakes.

For instance, within the poor countries, an earthquake may lead to the collapse of the entire nation. It's the case of Haiti, the poorest state on the American continent which, after the earthquake of January, 2010 (7.3 on Richter scale), collapsed almost irreversibly. If the epicentre of the earthquake is placed in the ocean crust, there can appear the tsunamis/tidal waves. In this situation, infrastructures on the coastal areas are literally pulverized. Depending on the nature of constructions, economic objectives and harbour facilities, there can occur the risk of explosions, fires, chemical or nuclear accidents.

Considered to be the most devastating in the last 100 years, the submarine earthquake produced on December, 26, 2004, in the Indian Archipelago (9.3 on the Richter scale), followed by tidal waves, provoked the deaths of about 228,000 people and massive damages to critical infrastructures (bridges, electricity and communications networks), harbour and touristic facilities. The waves propagated on extremely long distances (of over 4,000 km) affecting the shores of 10 countries.

The geophysical consequences of earthquakes at planetary scale are alarming. Post disaster calculations of the National Institute of Geophysics and Volcanology experts from Italy – quoted on march, 12, 2011 by News Agency ANSA[7], reveal spectacular moves of the Earth's rotation axis. After the quake in Japan (2011), the inclination of the Earth's rotation axis modified by 10 cm, after that of Chile (1960) by 8 cm and after the one of Sumatra, Indonesia (2004), by 6 cm. Because of these, the day time is shortened by 1-2 microseconds.

Consequences of the disasters on the electricity transport and distribution networks are extremely serious. There can be disrupted essential economic and social activities depending on electricity: medical emergencies and surgery blocks activities; laboratory refrigerators of all types; refrigerated warehouses; railway traffic; air traffic control; communications; emergency and public services. Also, in case of natural disasters, the IT infrastructure is specially vulnerable and might generate irrecoverable damages to all beneficiary sectors: finance and banking, energetic, transport, research, stock markets. The public utilities networks (water - sewage, heating, natural gas), themselves local critical infrastructures, are constructed in underground or laid above ground, on the street infrastructure. In case of earthquake, for instance, the public utilities network with pipes aligned to one another is endangered by the waving movements of the Earth crust and by soil liquefaction. There emerges the risk of some interruptions or/and damages (torsion and breaking of the pipes, connections, crossing elements) which would affect both crowded residential areas and the important economic operators (central heating, hydro- power dams, main gas transport and distribution networks etc.). Similar consequences - but at a much lower scale - are possible as well in case of landslides. During winter, the vulnerability of a community increases proportional to the degree of urbanization of the settlement. The damaging of the heat producing, transport and distribution may induce an important local crisis.

[7] *Cutremurul din Japonia a deplasat axa de rotaţie a Pământului*, 12 martie 2011, www.timpul.md/articol/Cutremurul din Japonia a deplasat axa de rotatie a pamantului-21405.html, accessed at 11.09.2014.

To conclude, we may say that during an earthquake all types of infrastructures are strongly affected or destroyed and the social and economic consequences are often irreversible. The energetic infrastructure is the most critical system under such circumstances, The interruption of electricity supply to consumers provokes major malfunctions in communications, industry, transport, medical services etc.

Volcano eruptions create vulnerabilities over wide communities and terrestrial areas. The leakage of incandescent lava on the slopes destroys constructions, elements of urban critical infrastructure and requires massive people evacuations. The huge smoke clouds, toxic gases and the ash spread in the atmosphere require urgent protection measures and people's evacuation or traffic limitations. Sometimes, eruptions are preceded, joined or followed by earthquakes which amplify the number of victims and the volume of damages.

Hurricanes (tropical cyclones) are extreme natural phenomena with weather and climate determination. Hurricanes are associated with storms and strong winds, localized near the Earth crust, which explains the dimensions of the damages suffered by communities (population, facilities, infrastructures).

Solar storms, through the negative effect of the electromagnetic flow are significantly influencing all categories of communications, including the air traffic control and the functioning of artificial satellites. There are more and more serious discussions about the disastrous effects of solar storms on electricity air transport networks. Such a phenomenon of cosmic origin may cause temporary interruption of the service on large areas, with serious consequences on today's society (medical services, communications, rail transport, aviation, utilities, industry). Prolonged droughts induce serious threats to energetic and food security. In the first situation, drought influences the river flows and, consequently, the diminishing of hydro power, sometimes to the breakdown level.

4. Human community resilience.

Resilience of every country, its capacity of managing a potential disaster, staying functional during the event and recovering after its ending reflects ultimately its level of development and organization of that society.

There are highly industrialized, urbanized and densely populated areas which are fully vulnerable in front of disasters. These megalopolises created, inevitably, functional infrastructures (electricity and gas distribution networks, underground and above ground roads and railways, cable transport, IT, telephone and heating networks etc) which can be interrupted under certain circumstances. The most illustrative example is represented by the energy falls in the summer of 1999 in the USA. The increased energy consumption caused by the high temperatures and the failing of equipment led to the blocking of 2,300 societies and of the Commercial Stock Market of Chicago. In Washington Heights (New York), more than 200,000 houses had no electricity for 18 hours. At Columbia Presbyterian Medical Center, many years' research and experiments on cancer and AIDS were compromised because of the failing of cooling equipment.

In order to quantify the resilience of a community/country it is necessary to analyse its coping capacity in front of sudden and violent manifestation of disasters. This concept combines the strategies and measures which act directly on the damages produced during an event by diminishing the impact or by adaptation strategies (behaviors which avoid the damage effects). The coping materialization implies creating of reply organisms and

capabilities, establishing of action procedures, creating proactive measures, preventive education of the population, efficient planning and timely resource mobilization. Resilience is, doubtlessly, directly proportional to the economic dimension of every nation.

Sequels of a natural disaster are different from one nation to another. If for a poor nation - Haiti, for example - damages in the amount of $ 2 million represent an immense effort to recover, for the USA it is an acceptable total.

Resilience includes coping. In other words, resilience expresses the measure in which one system has the capacity to absorb a disturbance (disaster) and recover easily after. Through its characteristics, resilience leads to sustainable evolution and to diminishing the vulnerability of a community.

At European level, for instance, in order that the EU answer in such circumstances to become more coherent and efficient, there appeared the necessity of a new strategy to approach the community aid quickly and efficiently for the countries affected by disasters. By Decision of the Council No. 2007/779/CE, Euratom, of Nov 8th, there was established the Civil Protection Community Mechanism. Its general aim is "to offer support, by request, in major emergency circumstances and to facilitate a better co-ordination of assistance interventions undertaken my the member states and by Community".

For Romania, the national critical infrastructure represents one of the main vulnerabilities and its protection is an essential priority, as it is mentioned in the National Defense Strategy (2010). The document says that 'the Romanian state has two ways to fight the identified risks, threats and vulnerabilities: by concentrating its own, national resources, and ... by co-operating with international allies and partners". In order to stress upon the necessity of improving the national resilience, the Strategy mentions that "any infrastructure inefficiently managed/protected may face critical moments marked by organisational crisis situations which might generate sudden, decisive changes, with negative consequences regarding national security".

In order to ensure an acceptable resilience in emergency situations, in Romania has been working since 2004 the National Emergency Situations Management System which is organised by the public administration authorities and which is composed of a network of institutions and organisms with responsibilities in emergency situations management, on levels and fields of competence. This system has the necessary infrastructure and resources.

Conclusions

Extreme natural disasters disorganize the whole system of critical infrastructures of a country. As a negative effect of dangerous hydrometeorological phenomena (abundant or long lasting rains, followed by floods, frost, strong wind, lightnings, snowstorms), geological phenomena (earthquakes) and geomorphological phenomena (land crashes and landslides), the essential importance belongs to the energetic system - the most critical infrastructure.

BIBLIOGRAPHY:

1. ALEXANDRESCU, Grigore; Gheorghe VĂDUVA, *Infrastructuri critice Pericole şi ameninţări la adresa acestora*, Bucureşti, UNAp/CSSAS, 2006.

2. BROWN, Lester R., *Starea lumii*, Editura Tehnică, 1999.

3. HOCIUNG, Cristian; Tudor HOCIUNG, *Captivi între infrastructuri critice*, Suceava, Editura Lidana, 2014.

4. OLSON, Peter, *Efectele mantalei interioare asupra geodinamismului*, 2003.
5.REPEZ, Filofteia, *Protecţia infrastructurilor critice - necesitate a prezentului*, Bucureşti, UNAp/ CSSAS, 2012.
6. NATO - Senior Civil Emergency Planning, Prague Summit, November 2002

E-sources:

1. *Nucleul Terrei se deplasează brusc*, 23.06.2008, http://www.descopera.ro/ dnews/2733343-nucleul-terrei-se-deplaseaza-brusc.
2. *Cutremurul din Japonia a deplasat axa de rotaţie a Pământului*, 12 martie 2011, http:// www.timpul.md/articol/cutremurul-din japonia-a-deplasat-axa-de-rotatie-a-pamantului-21405.html.

SOME CONSIDERATIONS ON THE DYNAMICS AND EVOLUTION OF MINORS' DISAPPEARANCES

Cristian-Eduard ŞTEFAN
Police Commissioner, PhD lecturer at the "Alexandru Ioan Cuza" Police Academy
of Bucharest and Director of the "Public Security Studies" journal.
E-mail address: cristian.stefan@academiadepolitie.ro.

Abstract: *The increased interest of the authorities for the minors' disappearances field is argued firstly, by the need to protect and respect the minors' rights, particularly vulnerable psychologically and socially. On the other hand, the disappearances of minors are events related with the specific issues of social environment where they live in, but also closely related to various forms of crime. In this study, I analyzed some general and specific aspects on the dynamics and evolution of minors' disappearances, aimed at strengthening the strategic and operational activities in this area.*

Keywords: *disappearance, missing minor, runaway, abduction, European Union, police.*

Introductive considerations

From the beginning, we have to mention that the disappearance of minors is a particularly current, in a continuous and evolving dynamic at an international, European and national level.

The actuality and the opportunity of this scientific approach circumscribes to the need to know and the need to analyze the current context of missing minors from the following perspectives: defining and circumscribing the phenomenons' visibility, especially in open sources of information, the typologies and its forms of expression, the quantitative dimension (statistics) of the phenomenon.

This study is based on a documented analysis of the existing data and information in open sources, in the products of the work of state institutions and nongovernmental organizations specialized in the field of missing minors, from the questionnaire data analysis applied in the countries in the field of missing minors, operational situation analysis on the dynamics and evolution of the phenomenon, and the data resulting from empirical research (fieldwork) performed in the operative units of the Romanian Police.

1. Analysis of the concepts and phenomena visibility

Knowledge of the dynamics and evolution of minors missing issues must proceed, according to the author, from a careful definition and delimitation of the concepts and terminology, assuming the working set - the dynamics and evolution of missing children. This work is required to identify a reasonable degree of approximation of the incidence of these cases in the international, European and national context, especially because there is no universally accepted international definition of missing children. Within this framework of analysis, we specify that the definition of specific work hypothesis is done by relating to general terms such as "disappearance" and "minor", and by reference to specific typologies of disappearance (voluntary departures, kidnapping, parental abduction, minor trafficking, disappearance with suspicions of murder, sexual exploitation, etc).

Without insisting on a theoretical and conceptual exam, we remember the fact that in most existing definitions in both inside explanatory dictionaries, and specific legislation and working procedures of police states and doctrine, we find the following common elements of the phrase "disappearances of minors":

a) statement about the general category of persons aged 18 years, including newborns subcategories, very small, small and adolescents.

b) the determining factor of establishing the disappearance is represented by the fact that the actual location where the child is not familiar[1].

c) there is no unitary definition of the term "juvenile disappearances" so: in some states, there is a legal definition of the term[2], in others the definition is done according to the content of police work procedures[3] or the work products of specialized NGOs; there are situations in which there is no universally accepted definition, but only based on the experience of practitioners in the field.

d) an observation with an universality character is that there are more frequent common definitions of particular categories of disappearance, than the phrase "missing juvenile", so we can easily identify the definitions of voluntary departure (flight minors), of abduction by a stranger, of parental abductions, of mysterious disappearances or the new challenges in this field, referring to disappearances of unaccompanied minors.

Public interest manifested for missing juvenile problems is quite broad, being shared not only by those who are directly involved (specialized institutions - police, non-governmental organizations - NGOs, parents and relatives of the disappeared minor), and also media and community members are involved, interested in solving these cases assessed as having a particularly emotional impact, due to the young age and vulnerability of minors, and the nature of possible consequences on their health and safety. This is due to, among other things, the existence of multiple online sources of documentation in this area, such as the websites of the International Criminal Police Organization Interpol and police states, which include public data and information concerning missing minors that are looked for (photo, marital status, distinguishing signs of the minors, etc.), specialized NGOs, various discussion forums and web pages or social networking websites in the field, some of them created by investigative journalists or even family members or friends of the missing persons.

The identification and research of the public interest in this area through open sources of information (online sources) has materialized through a search engine and online query or through Google Trends[4]. Thus, from the phrase "missing children" (translated into English, French, German and Romanian), from 2005 to 2013, we observe a high level of regional interest for online query in Argentina, Germany, France, Romania and the USA, a one moderate in South Africa, Switzerland, Austria, Ireland, UK, New Zealand and Australia, and a low one in Canada and Sweden. In this context, there was a high level of interest in Romania, especially in Bucharest.

---

[1] In this regard, we illustrate by presenting the following definitions, indicating that some of them refer to the general category of missing persons:

a) British Police defines a missing person as „any person whose location is unknown, whatever the circumstance of disappearance".

b) A study performed by the Australian Institute of Criminology (Marianne JAMES, Jessica ANDERSON, Judy PUTT, Missing persons in Australia, Australian Institute of Criminology, Violet Publishing Services, 2008, p.4) defines a missing person as „a person whose location is unknown, and there are serious concerns for its health and safety".

[2] See the Greek law, according to it „the disappearance of a minor can be a voluntary disappearance or a fact which results from takingthe minor from the place of its residence of the, independent of his will".

[3] Belgium has an operational definition of the missing person, stated in a ministerial decree according to which police must respond when a person is reported missing.

[4] This program monitors search interest for any topic - see website https://www.google.ro/trends. Please note that statistics are not absolute numbers of searches and online queries, but search volume from 0-100.

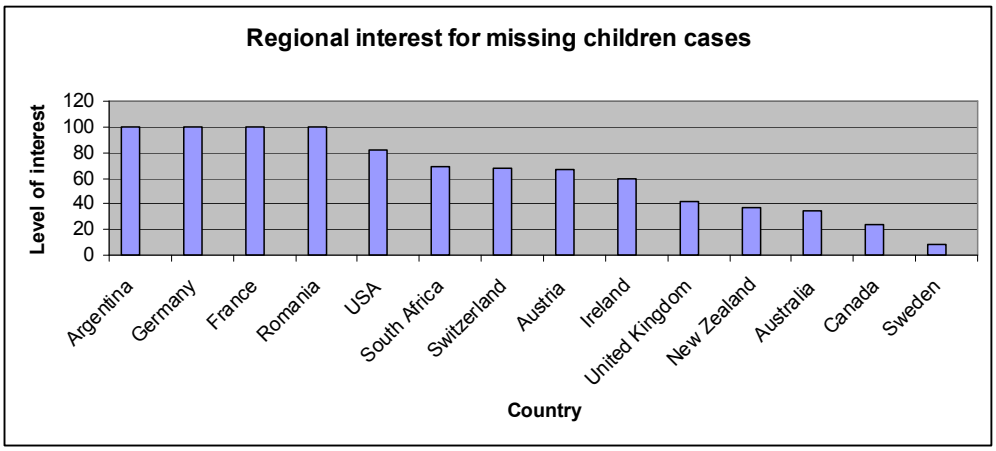


Figure no. 1. Regional interest for missing children cases (adapted from Google Trends).

3. Types and manifestations

Research and documentary analysis (monographs[5], studies and research[6], work products of various institutions, sources of online information, etc.) on the issue of missing juveniles led to the delineation of the following main types of disappearance:

a) voluntary departure (running away from home, residence or youth protection institutions[7]),

b) abduction of minors by unknown persons (third party),

c) parental kidnapping (national and international)[8],

d) disappearance of minors suspected of murder,

e) accidental disappearances of young children (products due to lack of supervision by parents - see cases of lost children, lost or drowned),

f) disappearances of unaccompanied migrant minors.

Of these types, the most common forms of disappearance encountered in international, European and national legal practice, are represented by voluntary departures of the minors - often determined by push and pull factors. Among these factors, the interviewed experts listed the lack of genuine communication between missing minors and their parents or care center representatives, the precarious financial situation of the minor's family, school dropout, negative influence of peers on the disappeared minor, and the spirit of adventure, libertinism, vagrancy etc.

However, as experts in this field indicate, voluntary departure may be a source of risk and danger to the health and safety of missing minors out of the supervision and parental authority or institution. Thus, there has been signaled the possibility of exploitation and sexual abuse, trafficking, involvement in prostitution, begging or other crimes.

Although statistically speaking, voluntary departures represent mostly disappearance cases, ending with the finding of the minors alive and healthy (without being the victim of a crime during extinction), we must not neglect cases and related conditions of alarming

[5] Gerard DESMARETZ, *Guide de recherche des personnes disparues*, Editeur Chiron, 2005.

[6] Gert VERMEULEN, *Missing and sexually exploited children in the enlarged EU. Epidemiological data in the new Member States*, Maklu Publishers, Antwerp-Apeldoorn, 2005; Stephen E. STEIDEL, *Missing and Abducted Children: A Law-Enforcement Guide to Case Investigation and Program Management*, National Center for Missing & Exploited Children, 2006.

[7] According to the work products of CRCDES Focus, annually there are recorded a significant number of missing children from foster care, and 20% of all cases investigated. See the Annual Report 2012, Romanian Center for Missing and Sexually Exploited FOCUS, p.8.

[8] In addition to this category, the 2011 Annual Report CRCDES Focus has revealed a new category of missing minors, where the child disappeared with one of the parents.

disappearances that generated the hypothesis of a kidnapping, trafficking, exploitation, sexual abuse of minors completed by murder even[9].

The analysis of the typologies and forms of manifestation of the alarming disappearance of minors[10], leads to the following operational classifications:

a) minors missing in mysterious circumstances (as defined by the interviewed experts as being suspect) that fall into the category of long-term disappearances - the current location of the minors is unknown, their body was not found and no other evidence, clues and reasonable assumptions about the commission of an offense,

b) children reported missing and were later found dead, most times the conclusion was that they were victims of sexual assault. This category is divided into two situations - on the one hand the criminals involved in the disappearance, beating and killing minors were identified and prosecuted, on the other hand, the murderer was not identified, these being the cases with unidentified authors[11],

c) cases of abduction of children by strangers.

The existence of cases of minors missing and later found dead (observing that they were victims of sexual exploitation and abuse offenses), determined in the author's opinion, the reorientation of the efforts of state authorities and NGOs in the investigation unit of the issues concerning missing minors[12] and sexual exploitation. In fact, the disappearances of minors are uncertain and ambiguous events notified to the competent authorities (police), especially when it is not a voluntary departure or a history of minor criminal or predelincvente. Experts of the Federal Bureau of Investigation (FBI) of the United States recommend that when investigators are in front of a mysterious case of disappearing (without direct evidence, no witnesses and no history of voluntary departure of the minor), to issue from the start the hypothesis of abduction of the minor[13].

One of the new challenges in the field of missing minors in the European context is the disappearance of unaccompanied migrant minors. Although the Romanian government has not been facing (fortunately) so far with such events, other countries deal with this situation as a real resurgence. Thus, in the UK, approximately 60% of unaccompanied migrant minors accommodated in centers and health care disappear and are no longer found. The Swiss authorities have recently reported the existence of cases of unaccompanied migrant minors trafficked by criminals from Africa. In Belgium, according to the organization Child Focus, officially, there is a high number of cases of disappearance of unaccompanied migrant minors, but it is estimated that there is a "black figure" of this category of minor missing which is not recorded and reported to relevant authorities.

Another challenge is the parental kidnapping (national and international). Although in our country such cases are rare, some of which were not reported to police, but by civil way,

---

[9] In close connection with this, a recent study of ICMEC (citing an analysis of Justice Department of USA), on the disappearance of minors in Central America, points out that „juveniles and adolescents who run away from home or are abducted are vulnerable and face high risk situations, such as sexual exploitation, human trafficking and prostitution, involvement in criminal activities - as a victim or offender, physical and emotional health damage, risk of physical and sexual abuse, and sometimes their killing". See for details in Missing Children in Central America: Research of Practices and Legislation on Prevention and Recovery, United Nations Children's Fund (UNICEF) & International Centre for Missing & Exploited Children (ICMEC), 2011, p. 7.

[10] Categorizing alarming disappearance is based on the existence of certain specific circumstances such as the age of the disappeared minor, if there are medical problems or disabilities etc.

[11] Although statistically speaking, these cases are exceptions and are extremely rare, they have led in most cases to killing of missing and sexually abused minors, causing outrage among the public.

[12] For example, the organization Missing Children Europe includes in the category of child sexual exploitation and abuse, the following types of crimes: abuse or sexual assault, child prostitution, child pornography, child trafficking for sexual exploitation and grooming (online recruiting children).

[13] Child Abduction Response Plan. An investigative guide, US Department of Justice, Federal Bureau of Investigation.

others face the existence of international parental abduction, especially in the context of the existence of mixed marriages (which include couples of different nationalities and mentalities). Situations of this kind, as experts stated, don't have as a feature the aggression of the disappeared minor, only that the location of the minor is hidden to the caregivers or legal representatives.

4. The extent of missing minors

The cause of the statistical dimension of the phenomenon of missing minors was based on the study and analysis of statistics (operational situation) of the police of different countries and different institutions like NGOs.

Please note that these statistics differ[14], depending on the organization that is the source of the statistics, the method of collecting and recording of data, and the existence of cases of disappearance that police are not notified of or are not recorded as extinct.

In this respect, the analysis of online sources of information, activity products (reports, studies, public information, etc.), highlights the existence of various categories of statistics regarding the phenomenon as follows:

- Statistics of national police units, some with public character, other confidential,
- Statistics of NGOs specializing in issues of prevention and combating missing juveniles[15],
- Statistics regarding the number of alerts concerning Schengen type missing minors, introduced in the Schengen Information System.

Also, there is lack of a unified tool for monitoring and recording statistical annual disappearances, which are different from case to case.

According to information published by ICMEC on the official website of the organization[16], worldwide are reported missing about 8 million juveniles annually, of which 800,000 are minors in the United States of America (USA), 230,000 cases in the UK [17](from 2009 -2010), 100,000 cases in Germany, 50,000 in Canada[18], 45,000 in Mexico, 40,000 in Brazil, 39,000 in France and 20,000 in Spain. Accumulation of annual statistics of disappearances published by the representatives ICMEC leads to a discrepancy with statistics recorded at European level.

---

[14] According to the organization Missing Children Europe, the lack of reliable data at European level on the disappearances of minors should not allow underestimating the problem.

[15] As shown in the analysis of annual reports of CRCDES Focus 2010-2012, casuistry dealt with by specialists statistics office does not match existing records of Romanian Police, a possible cause is shown by the fact that not all cases of disappearance of minors are notified to the police, and are subsequently submitted to the CRCDES Focus. Mainly the complaints coming from CRCDES Focus are received through European emergency line for Missing and Sexually Exploited 116,000. Focus CRCDES NGO statistics on the number of incoming calls is not just the registration of new cases of child missing, but the evidence regarding the presence of the minor disappeared in a certain area and requests for information/assistance. See the Annual Report 2011, the Romanian Center for Missing and Sexually Exploited FOCUS.

[16]International Centre for Missing and Exploited Children Overview, http://www.icmec.org/en_X1/icmec_publications/ICMEC_mech.pdf, last accessed 1 September 2014.

[17] This statistic does not correspond to the figures presented by the Home Office. In the breakdown of total annual disappearances of minors in the EU, at Member States level, in the UK, according to a 2010 report of the Ministry of Interior (The Home Office), are notified annually 140,000 cases of missing minors and nearly 383 cases/day.

[18] In Canada, according to data presented by the Missing Children Society of Canada association, the statistics in this area are alarming and does not reflect the exact figures being higher. The first statistics on missing minors were offered advertising in Canada in 1987. As of 2013, there were 41,035 cases, including 29,871 cases of voluntary departures, 9147 disappearances of unknown origin, 77 with parental kidnapping custody and 33 cases of abduction by a third party. See http://www.canadasmissing.ca/pubs/fac-ren 2013-eng.htm#id, last accessed 28 August 2014.

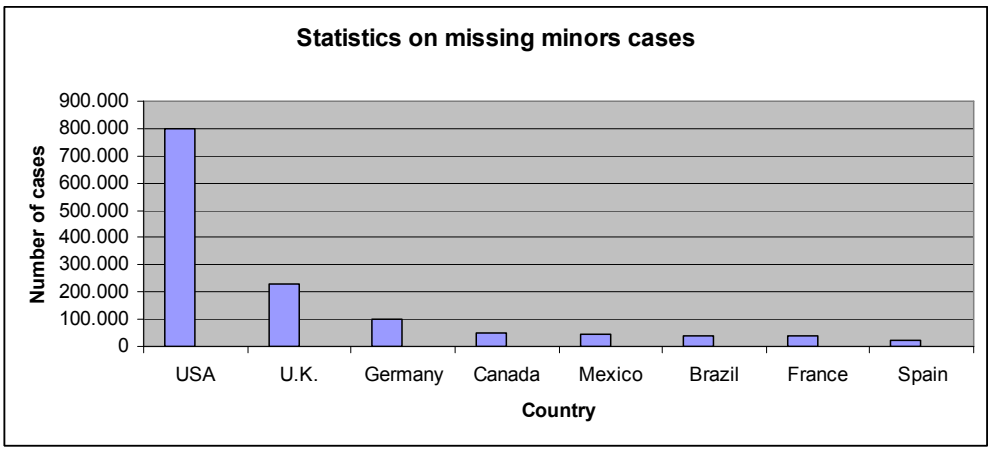


Figure no. 2. Country statistics on missing minors cases (Source: ICMEC).

On the other hand, the authorities of the Russian Federation issued in 2010 a figure of 19,734 missing juveniles nationwide[19], including 5,219 under the age of 14 years, while in Australia about 20,000 minors disappear every year[20].

In contrast, in the EU, according to the European Commission, every two minutes a minor is declared missing, statistical milestones leading to an annual 250,000 missing juvenile in the EU.

In the period 2012-2013, at the request of the Directorate-General for Justice of the European Commission, a study was conducted by the Association of ECORYS Nederland BV, concerning data collecting and statistics on missing children in the EU. Comprehensive study was conducted in the Member States, data being collected through the national police and NGOs, as well as from interviews conducted with various specialists. Information collected by the Dutch association lead to general and specific statistics on the missing children, as follows: disappearance statistics by gender or age of the child, the number of cases brought by 116,000, the number of international abductions, voluntary departures (including institutions protection of minors) sensed unaccompanied migrant minors missing etc.

Country / Year of disappearance	2008	2009	2010	2011	2012
Belgium	462	388	334	420	315
Bulgaria	1270	1175	1247	1230	1276
Czech Republic	7937	7490	6715	6547	5564
Denmark	1102	1135	1006	911	1039
Germany	35249	34889	36732	39708	42943
Ireland	No data recorded	5614	6141	6360	6615
Estonia	2	5	1665	4581	13006

[19] Investigating crimes against children one of priorities for Investigative Committee, The Investigative Committee of the Russian Federation, http://www.sledcom.ru/blog/detail.php?ID=50615&sphrase_id=71702, last accessed 5 September 2014.

[20] Working with young people, Australian Federal Police, National Missing Persons Coordination Centre, http://www.missingpersons.gov.au/education--training/working-with-young-people.aspx, last accessed 11 September 2014.

France	47910	47491	48202	52742	50326
Italy	4752	3817	3645	5396	5513
Cyprus	No data recorded	68	92	62	No data recorded
Lithuania	90	866	929	1152	1288
Hungary	11901	11876	12053	14419	No data recorded
Netherlands	89	104	160	202	261
Poland	4168	3625	3471	4351	6453
Portugal	2904	3087	3552	3120	2973
Romania	3362	3243	3124	3182	3199
Slovakia	1554	1456	1476	2139	1821
United Kingdom	66188	83483	100189	91230	96341

Table no. 1. Missing minors cases in 18 EU Member States
(Source: Missing children in the European Union. Mapping, data collection and statistics, European Union, 2013.)

As shown, the total number of missing minors in 18 EU Member States analyzed varies, from a figure of 188,940 cases in 2008, followed by an ascending curve, the peak being in 2011 (with 290,494 cases), followed by a decrease, respectively 238,933 cases in 2012.

Europe's Missing Children Organization NGO is specialized in missing minor issues, which is made from the adhesion of 30 organizations from 25 European countries. According to statistics of the organization, between 2 and 5% of disappearances of minors are abductions by third parties, while the case of fugitives is in over 50% of cases reported to hotline of specialized NGOs sites[21]. Also, 12,690 unaccompanied minors sent a request for asylum in the EU in 2013.

In Romania, the disappearance of minors is an issue that is taken under consideration and concern by many institutions and authorities. Thus, in terms of investigative solving missing minor research, the competence is under the judicial police of Romanian Police, which according to the tasks set by the Law no. 218/2002, conducts activities of missing persons, including minors missing. Police activities in this field are complemented by additional intervention of NGOs specializing in this field, especially Romanian Center for Missing and Sexually Exploited Children (CRCDES) FOCUS, whose purpose is the initiation of efforts to prevent and resolve cases involving missing or sexually exploited children. At the same time, they have skills in different segments, and have specialized structures that support children's rights and child protection, prosecution composed of prosecutors specialized in investigating crimes against life and other collaborative partners, based on the conclusion of agreements and protocols.

Statistics on juvenile disappearances are made both by Romanian police, and the CRCDES FOCUS, with the observation that they differ, the CRCDES FOCUS statistics are made primarily on cases brought before the hotline 116 000.

According to existing statistics from the General Inspectorate of Romanian Police (IGPR), juvenile disappearances recorded an upward trend since 2006-2007, when there were 1,348 and 2,848 cases, moving to a constant figure of over 3,000 cases of disappearance (from 2008 to the present). It should be noted that a very high percentage (over 90%) of this category of missing minors, are found and removed annually from police records, remaining

[21] Missing Children Europe Annual Report 2013.

constant, a figure of about 300 minors missing (some of them long disappeared category duration).

Year of disappearances	Number of cases of missing minors
2004	236
2005	344
2006	1348
2007	2848
2008	3368
2009	3243
2010	3124
2011	3182
2012	3199
2013	3483

Table no. 2. Number of cases of missing minors in Romania for 2004-2013 (Source: The General Inspectorate of Romanian Police).

The explanation for the increased number of cases of child missing every year in Romania, according to the representatives of the Romanian Police, consists mainly in the fact that the current registration receipt of the referral and case investigation disappearing, implies an immediate response from police, search activities the minor disappeared immediately starting. However, prior to 2006, it is possible that minor differences could be found within 48 hours after the disappearance, in which the referral of extinction and commissioning follow the minor is made after the passage of 48 hours. Meanwhile, police interviewed stated that the annual statistics of missing minors in Romania include the number of cases reported and notified to the police, with cases of minors who repeatedly left home or care facilities, each departure being registered as a new species.

At the level of IGPR, as specified by specialists of the Romanian Police, there isn't a database designed strictly for juvenile cases or missing persons, which are highlighted in the content of the application Wanted, therefore with other people who are wanted - wanted person under of arrest warrants, EAW, etc.

Also, the experts interviewed also reported that police databases revealed statistically the number of people missing in a given period of time, without custom categories and particular extinction typologies - juvenile runaways, abducted, drowned etc.[22]

Conclusions

Diagnosis phenomenon of missing minors requires detailed knowledge of the following sizes - delimitation of categories of disappearance and of children reported missing, the identification of the causes and factors that lead to disappearances and the most effective ways to prevent and combat disappearances in the case of collaboration between inter-agencies in this field.

The prevention and combating of minors' disappearances, especially the alarming ones related to various forms of organized crime, constitutes an internal security problem. The protection of minors against all forms of disappearances and exploitation represents an essential aspect of the national security strategies of every state, especially in the context of

[22] Analysis of the annual reports of CRCDES FOCUS highlights the existence of more comprehensive statistics and records detailed in this respect is highlighted: the distribution of cases by type of extinction, area of origin, depending on the severity, endangered environment (urban / rural), by gender, level of education etc.

prevention and combating organized crime. The application of minors' protection forms consolidates the trust in public institutions, regarding the implementation of the internal security strategies.

One of the problems identified during the research conducted by the author refers to the lack of data and information on trafficked minors (in the context of child trafficking for sexual exploitation, labor exploitation, for begging, etc.) in the category of missing. These results both from interviews with synthesis specialists in Romanian Police, and documentary analysis. The answers were referring on the one hand, to the inadequate collaboration between structures and institutions, but also because the exploitation of the victims usually takes place in a other country than the native country, or the victim does not press charges against traffickers, which strengthens the claim practitioners that "If you don't have a victim, you don't have human trafficking".

Consequently, in conjunction with the latest statistics conducted internationally, we deduce the following conclusions:

a) At an international level, there are approximately 250,000 missing juveniles annually and two million trafficked minors for different purposes (according to UNICEF, 2007).

b) based on this finding, practitioners do not exclude the hypothesis that children still missing and unaccounted for (so-called long suspicious disappearances) have been victims of child trafficking, and that the category of trafficked minors and minors find themselves missing, especially in the category of minors flee from home or care facilities.

Assertion author correlates with the Commission's concerns from recent years to identify possible links between human trafficking and sexual exploitation of children, in general, the issue of missing minors, especially disappearances high risk (such as abductions). In this respect, we mention a recent statement of the EU anti-trafficking Coordinator dr. Myria Vassiliadou that says "minors missing is a vulnerable group to human trafficking".

Finally, experts in this field think that there is a need to build databases and official records that are more comprehensive and relevant for missing juveniles, to have a clear and unified vision of the phenomenon.

Acknowledgement:

This work was made possible with the financial support offered through the Development of Human Resources Sectorial Operational Program 2007 - 2013, co-financed through the European Social Fund, within the project POSDRU/159/1.5/S/138822, entitled ***"Transnational Network of Integrated Management of Intelligent Doctoral and Postdoctoral Research in the "Military Sciences", "Security and Information" and "Public Order and National Safety" Domains - a Professional Training of Elite Researchers Programme - "SmartSPODAS"."***

BIBLIOGRAPHY:

1. DESMARETZ, Gerard, *Guide de recherche des personnes disparues*, Editeur Chiron, 2005.
2. JAMES, Marianne; ANDERSON, Jessica; PUTT, Judy, *Missing persons in Australia*, Australian Institute of Criminology, Violet Publishing Services, 2008.
3. VERMEULEN, Gert, *Missing and sexually exploited children in the enlarged EU. Epidemiological data in the new Member States*, Maklu Publishers, Antwerp-Apeldoorn, 2005.

4. *** Missing children in the European Union. Mapping, data collection and statistics, European Union, 2013.
5. *** Missing Children Europe Annual Report 2013.
6. *** Missing Children in Central America: Research of Practices and Legislation on Prevention and Recovery, United Nations Children's Fund (UNICEF) & International Centre for Missing & Exploited Children (ICMEC), 2011.
7. *** Annual Report 2012, Romanian Center for Missing and Sexually Exploited FOCUS.
8. *** Annual Report 2011, Romanian Center for Missing and Sexually Exploited FOCUS.
9. *** International Centre for Missing and Exploited Children Overview, http://www.icmec.org/en_X1/icmec_publications/ICMEC_mech.pdf, last accessed 1 September 2014.
10. *** Investigating crimes against children one of priorities for Investigative Committee, The Investigative Committee of the Russian Federation, http://www.sledcom.ru/blog/detail.php?ID=50615&sphrase_id=71702, last accessed 5 September 2014.
11. *** Working with young people, Australian Federal Police, National Missing Persons Coordination Centre, http://www.missingpersons.gov.au/education--training/working-with-young-people.aspx, last accessed 11 September 2014.

STRATEGIC CULTURE'S ISSUES IN MAPPING A DYNAMIC SECURITY ENVIRONMENT

Răzvan George ŞTEFAN
PhD, "Mihai Viteazul" National Intelligence Academy,
Bucharest, Romania.

Abstract: *Globalizing vulnerabilities, risks, threats, dangers and agressions to whose drivers are not only state actors, but also groups or individuals organized in international networks, led to the reconfiguration of security strategies and adapt them to provide an effective response to the challenges of the contemporary security environment.*

Competition for soft power takes place both in the states and individuals. Between these two areas, there are influences, interrelationships, some clearly visible, others diffuse volatile. The state continues to be responsible, according to classical political theory, for the welfare of their citizens will need to refer to them in the legitimacy of governance and prioritizing its domestic or foreign affaires.In the other hand, the individual, community, network become storage of a power that can not only influence the policy of a state, but also could substitute for domestic power centers, they can challenge state authority or even acquire its own geopolitical relevance globally.

The 21st century is an era of change. The globe is under the influence of three major world trends: the revolutionary development of information and communication technologies, the transition to a knowledge society and the new learning mode of the Net Generation. These trends have generated a shift in the self-security paradigm of nations, giving rise to the need to cultivate new competencies for citizens, professionals, decision-makers in knowledge society.

Keywords: *soft power, knowledge-centric, knowledge society, adaptability, transperancy, accountability, partnership strategy.*

1. Looking to understand new strategic values

1.1. Think globally and act locally

The philosophy behind the building of the international security environment over the past century has suffered a transformation. Transformation is a process that occurs naturally in the continuous adaptation of strategies in relation to the event's dynamic, constantly pursuing goals in a related area.

Accelerating globalization has resulted in more opportunities for development and global cooperation and also to the exponential growth of the number of entities that operate in the global arena. In this context the decision-making process in foreign policy and security of states and international organizations has become increasingly complex.

The danger of terrorist actions anywhere in the world and the begining of the war on terrorism has led the repositioning of actors in the international security environment according to their own interests, some publicly acting to combat this phenomenon and others tolerating or encouraging terrorist activities.

The concept of strategy is closely related to the concept of strength, defined as the ability and capability to produce the desired effects. In the modern world this ability is mainly based on two pillars:military power and economic power. In a broader sense we can consider that the information, resources, technology, culture and education and other basic elements

that create the foundations of power subscribe or depend to varying degrees by economic pillar.

Given that to situations in dynamic domestic and international security environment,when the power, as we have defined it above, can not respond effectively to challenges, issues arising in the security environment or simply do not provide fulfilling the interests of the nation, here is the role of strategy to organize the components of power, to distribute resources optimally to achieve goals in a certain area.

Strategies' quality and their practical value depends largely on the ability of a nation's decision makers to understand and predict the dynamics of internal or external circumstances, factors influencing the effective use of power in a particularly sense. The strategy is a matter of choice. The most valuable strategies are those who correctly anticipating developments and set proper measures in relation to them. Positive and negative dynamics must be prevented with proper measures to boost efficiency or to reduce loss. The strategy brings together a set of options to respond in a certain way to a situation or a plurality of situations.

The review and development process of a new security strategies in the Western countries is part of a larger phenomenon that occurs globally and is seen in the development of overall, systematic and long term reforms in this field. These redefinitions is a national priority of the new security and intelligence strategies and targeting strands such as: coordination, structural changes, formation of a new structures, improving the quality of human resources and business reform in the field of intelligence research, developing technical capabilities in intelligence collection. All these directions and actions are deemed necessary to prepare a strategic shift in the intelligence world to meet the new challenges of the XXI century.

The changing character of conflict will continue to evolve over the next 20 years as potential combatants adapt to advances in science and technology, improving weapon capabilities, and changes in the security environment.

Warfare in 2030[1] is likely to be characterized by the following strategic trends: *the increasing importance of information* (advances in information technologies are enabling new warfighting synergies through combinations of advanced precision weaponry, improving target and surveillance capabilities, enhanced command and control, and the expanding use of artificial intelligence and robotics)[2], *the evolution of irregular warfare capabilities* (the adoption of irregular warfare tactics by both state and nonstate actors as a primary warfighting approach in countering advanced militaries will be a key characteristic of next conflicts)[3], *the prominence of the nonmilitary aspects of warfare* (non-military means of warfare, such as cyber, economic, resource, psychological, and information-based forms of conflict will become more prevalent in conflicts over the next two decades)[4], *the expansion and escalation of conflicts beyond the traditional battlefield* (the advancement of weapons capabilities such as long-range precision weapons, the continued proliferation of weapons of mass destruction, and the employment of new forms of warfare such as cyber and space warfare are providing state militaries and nonstate groups the means to escalate and expand future conflicts beyond the traditional battlefield).

---

[1] ww.dni.gov/nic/NIC_2030_project.htm.

[2] By 2030 some states probably will deploy weapons designed to destroy or disable information, sensor, and communication networks and systems including anti-satellite, radiofrequency, and laser weapons).

[3] Modern communication technologies such as satellite and cellular phones, the Internet, and commercial encryption, combined with hand-held navigation devices and high-capacity information systems that can contain large amounts of text, maps, and digital images and videos will greatly enable future irregular forces to organize, coordinate, and execute dispersed operations).

[4] In the future, states and nonstate adversaries will engage in "media warfare" to dominate the 24-hour news cycle and manipulate public opinion to advance their own agenda and gain popular support for their cause).

1.2. Flexible, innovated and future oriented atitude

Strategy is hard to do, because it is both an art and a structured intellectuall process. It is the constant adaption of ends and means to shifting conditions, in an environment where chance, uncertainty, fog, friction, and ambiguity dominate. To make it even more complex, strategy is a multi-sided affair: the objectives, intentions, actions, and reactions of other participants – both allies and opponents – are often opaque and varied. National interests and policy goals play a critical role, as do diplomatic, financial, technological and military resources. Other factors, such as history, culture, ethos, and personalities, all influence strategic behavior in subtle, but significant ways. In today's globalized world, driven by a 24/7/365 news cycle, these realities require a broader, more integrated, less linear approach.

The twenty-first century strategist's task demands that it be approached in the context of its environment, factoring in a vast array of dynamic and increasingly complex variables. Strategy is not developed in a vacuum. Any use of force is, ultimately, a political act. Military power must be considered and evaluated in tandem with other instruments of statecraft, as well as public-private interfaces. This task requires rigourous, precise thinking and the ability to reconcile or choose among a spectrum of competing options. There are no easy answer to guide the strategist along, except the knowledge that the only alternative to a holistic approach is inconsistency, wasted effort, delayed decisions and increased risk.

Strategic succes is built on four mutually supporting pillars: grasp of strategic theory and historic practice; innovation, integration and alignment.

The function of any theory is to describe, organized and explain a body of knowledge. Strategic theory has an added function: it guides action. Thus, it is nothing but pragmatic. To quote one America's foremost strategists, Bernard Brodie: "Strategy is a field where truth is sought in the pursuit of viable solutions". Therefore, all strategies seek to optimize available means to achieve the desired ends with acceptable risk.

Innovation is the ability to think anew and capitalized on changed circumstances – the fusion of creativity and logic, some innovations involve science and technology, while others are in realm of concepts and organizational design. In all cases, the ability to innovate rests on foresight – the aptitude to read both current and emerging trends, as wll as to anticipate their impact. Innovation also requires courage, perseverence, entrepreneurship and readiness to "break glass", especially in large bureaucracies and across sector boundaries.

Troughout history, some leaders have chosen to stick with comfortable assumptions and time-tested constructs, failing to realize that the strategic environment within which they function fas been fundamentally transformed. Other leaders have managed to exploit the potential for innovation, fusing new concepts, technologies, approaches and organizational structures into overwhelming combinations of effects. Their gift was integration and holistic thinking.

Integration is the ability to "connect the dots" and relate seemingly disparate activities to one another. Absent integration, second and third order effects are difficult, if not impossible, to anticipate. Holistic thinking is an approach that captures both the whole and its parts, allowing one to grasp multi-dimensional, dynamic relationships as they are today and as they might evolve tomorrow. It prepares the practitioner to foresee a wide array of potential consequences, yet neither assumes nor expects perfect congruence or linearity. Without integration and holistic thinking, one would be a permanent victim of surprise, reacting haphazardly to unanticipated, seemingly random events.

All strategic designs must be integrated horizontally and vertically. The best plan, even if flawlessly executed, will fail if its implementation does not support the over-arching objectives. Likewise, a lofty strategy unsupported (or unsupportable) by operational or fiscal realities is, at best, an academic exercises or, more often, a prescription for disaster.

Alignment and *coordination* within and among military servicies and government agencies, and with the private sector, produce synergies, save lives and enhance strategic effectiveness. They are predicated upon and reflect trust and confidence in each other's capabilities, as well as an in-depth understanding of and ability to compensate for their inherent limitations.

In sum, strategy is the product of imagination, creativity and sound logic. Effectiveness comes from an integrated, synchronized effort, sustained over the long-term and guided by a clear vision of the desired end-state.

Against this backdrop, surprise is a strategic discontinuity, a startling seismic shock. It upends best laid plans, unbalances a comfortable posture and gives a whole new meaning to the adage that "the opponent gets a vote". Surprise causes psychological dislocation and at least temporary paralysis: one is no longer driving events and is forced, instead, to respond in and to an environment shaped by another's actions.

2. Repositioning to enemies' horizonts

Throughout history, leaders at all levels have operated with limited information and constrained situational awareness. Today, decision-makers are suffering the embarrassment of riches, virtually drowning in data delivered at a velocity and volume far exceeding their ability to absorb. Nations must continue to develop systems that are not just network-centric, but knowledge-centric. These systems would integrate data in a manner consistent with natural neurological patterns, presenting information in a format that enables timely, logical decisions. To this end, we must fully harness the power of machine-to-machine interface, freeing up human resources for activities where intellect and esprit remain indispensable.

In the other hand, there's two failures that are occurring in the world: failure of nations states and failure of governance.

When you look at different parts of the world, they are being challenged by this rise of corruption. And we have to recognize that because rich countries invest in places where there's a lot of corruption, where there's kleptocrasies. We have to recognize that! So, what do we need to do?

A very interesting and recent point of view has been released by an important USA's intelligence leader[5]: "We need to have an enormous agility as a nation to be able to operate in the different environments that we are in. Agility is something that allows us to be/to move at a relative speed that's good and helpful for what it is that we've trying to do. We need to be very adaptative. We need adaptability. Transparency is a big word that came up a lot today. Transparency breeds trust. And from an intelligence, we cannot afford to lost trust. Transperancy has to be a sort of a watchword for the intelligence community and certainly for everything we do. Accountability. We have to be accountable for what our actions, we got to be accountable for the thing we do, what we say and how we want to be. And the last comment is that, I just wrote down that stability is only temporary without good governance. Unless you have good governance you really can't have stability".

Perhaps the best known and certainly the most influential concept that expresses the nature of power in the context of the interaction changes the centripetal forces of the information age is that of "soft power" by Joseph Nye, focused on the notion of "credibility" on the international scene, as a factor of acceptance and not coercive. But also the credibility is distributed unevenly among the actors who hold it, being built on the ability to access

[5] Lt. Gen. Michael Flynn, Director, Defense Intelligence Agency USA, interviewed in Aspen *Institute Homeland Security Program 2014*, section *The Global Threat Picture as the Defense Intelligence Agency Sees It*, 26 julie 2014, to be wached at *http://aspensecurityforum.org/media/live-video/*.

information on understanding and its use. There is a kind of "asymmetry of credibility" that, beyond a certain critical level, it may acquire, under certain circumstances, even scale of a power factor.[6]

Competition for *soft power* takes place both, at the states and individuals levels. Between these two areas, there are influences, interrelationships, some clearly visible, others diffuse volatile. The state continues to be responsible, according to classical political theories, for the welfare of their citizens, so will need to refer to them in the legitimacy of governance and prioritizing its domestic or foreign goals. *In the other hand, the individual, community, network become storage of a power that can not only influence the policy of a state, but also could substitute for domestic power centers, and they can challenge state authority or even acquire its own geopolitical relevance globally.*

The picture is more complex and serious than it would bode this sentence. We talk about crime networks, rebel groups, terrorist organizations, failed states, nation states with hostile intentions - all unleashed in a virtual space, like any tool, allows use both legitimate and evil way. Even worse is that none of these attacks can be seen with the naked eye. They can not be charged with a sixth sense, or understood without a significant effort from the private user or state institutions, some of them taken by surprise by the waterfall and technological hazards arising from it.[7]

3. Knowledge society - a smart shield against volatile threats

3.1. Rising of a new society

Recent studies[8] have indicated that future society will comprise the semantic Web, Big Data, cloud computing, smart phones and apps, the Internet of things, artificial intelligence and various new gadgets. In short, it will be an *information and communications technology* (ICT)-based society.

The following key future competencies, classified into three categories, are identified as essential to future society:

- ✓ conceptual competencies: connectivist thinking, innovative thinking and problem solving, critical thinking, reflective thinking and positive thinking skills;
- ✓ practical competencies: media and information literacy (with ICT skills as a key component) and learning skills;
- ✓ human competencies: social networking skill and virtual collaboration, self-management, humanistic consciousness, digital citizenship and cross-cultural interaction skill.

It has been found that access to information has improved as ICTs have developed, most notably in relation to the growth of mobile phone use. Mobile phone use in developing countries has created a “leapfrog” phenomenon that enables millions more people to access the information society. Although a digital divide still exists amongst countries and marginalised social groups, attention has shifted from material access to actual use and application, which has been coined the “digital use divide”. Freedom of the press has not exhibited much improvement in the past decade, but the emergence of “we media”, such as social media and blogs, has offered ordinary people unprecedented opportunities to express their views and contribute to media pluralism.

---

[6] Ambasador Maior, George Cristian, *State, reţele, companii şi indivizi: paradoxurile spaţiului cibernetic*, în volumul *7 Teme fundamentale pentru România*, Ed. Rao, Bucureşti, 2014, pag. 191.

[7] Ambasador Maior, George Cristian, *Cuvânt – înainte* , în volumul *7 teme fundamentale pentru România*, Ed. Rao, Bucureşti, 2014.

[8] Alice Y. L. Lee, *Literacy and Competencies Required to Participate in Knowledge Societies*, in *WSIS+10: Overview and Analysis of WSIS Action Lines C3 Access to Knowledge and C9 Media*, accesed at http://www.wsis-community.org/ pg/ groupwiki/ owned/group:15325.

Other enablers in the implementation of ICT movement, the groundswell movement, the multi-stakeholders' approach combating the global digital divide, citizen journalism, education reform, mobile technology adaption and the strong sense of social justice upheld by the Net Generation. Barriers and challenges remain, generated by the global digital divide and a lack of access to ICTs, race, gender, age, disability, language and political instability, in addition to restrictions in freedom of the press rooted in political reasoning and media concentration.

Recommendations for tackling these issues include:

- ✓ maximising mobile technologies and promoting m-learning;
- ✓ cultivating 21st century competencies with objectives such as responding to the specific needs of the new socio-technological environment, narrowing the "digital use divide", fostering media pluralism and contesting restrictions on freedom of speech;
- ✓ establishing collaborative networks and strategic partnership;
- ✓ education reform and Teacher Training;
- ✓ contextualising initiatives for specific cultural settings;
- ✓ considering the power of individuals (particularly the Net Generation) in the civil society when suggesting that more research should be conducted in this respect.

3.2. Knowledge tools that gives strategic advantage

There are some propositions intended to guide soldiers, diplomats and decision-makers at all levels, as well as those who support the endeavor to remain even vigilant in providing for the common defence[9]:

- ✓ always conduct a reality check from not only your own perspective but also that of the opponent. Reality always has rough edges, ambiguities and shades of gray. If everything is crystal clear and consistent with your best case scenario, circumstances, you are probably being deceived.
- ✓ state assumptions clearly and explicitly. Identify pivotal assumptions, those that if proven wrong would upend your entire approach. Develop a system to periodically revalidate these assumptions, making sure you don't confuse estimates with facts or hopes with viable courses of action. Remember that any plan that relies on more than two consecutives miracles and violates more than one law of physics is not suitable – even as a deception or feint.
- ✓ don't fall in love with any plan, policy, program or assessment. Don't expect the opponent to cooperate. Have a branch and sequel to address the unexpected along the lines of "what if?" and "what next?". Pay attention to what both adversaries and allies are saying and doing – especially if there is a mismatch between words and deeds. Don't discount indicators just because they point to things you would never do. There are no universal standards of rationality or recklessness.
- ✓ collaborate with all who might provide fresh insights and different perspectives. Keep this circle as diverse and wide as practicable. Help your colleagues by asking the "right" questions. Tell them explicitly is capable of assessing intentions. Question the "bona fides" of any informations – no matter how comforting, convincing or highly classified.
- ✓ you don't know what you don't know and you don't know can spell disaster. Create an organizational climate that allows for alternative viewpoints to be given a fair hearing. Beware of group-think and remember that just because something never happened before does not preclude it from happening. Every precedent was created by someone's act of courage or folly.

[9] Lani Kass/J.Phillis London, Surprise, deception, denial and warning: strategic imperatives, 2012, Forign Policy Research Institute, winter 2013, orbis

✓ trust your instincts and be ready to pay the price that might go with that. Warning is about being safe, not about being right. Beware of the "cry wolf" syndrome, but don't dismiss the bearers of bad news. Sometimes the wolves are really at the gate and "inflammatory rhetoric" indicates a real and present danger.

✓ timely, unambiguous warning is nice to have, but don't count on it. Don't assume or expect that appropriate decisions, authorities and actions would automatically follow. You have plenty of latitude within your own organization. Do what's right, even if you have to stake your career on it.

✓ don't be a victim! It's painful, even if you ultimately win. Never allow the initiator to exploit his initial success. Surprise only determines where and how the first battles will be fought, but it's up to you to revalidate this principles every single time.

✓ guide is neither the opposite of valor nor an effective substitute for capability and capacity, but it saves lives and treasure. It is an asymmetric advantage we forfeit to others at our own peril.

All strategic planning is based on a set of assumptions. Surprise occurs when core assumptions are proven wrong. History is replete with examples of militaries and intelligence communities that failed due to their inability to validate assumptions, adopt new concepts, transform organizational culture, or leverage breakthrough technologies. But militaries and intelligence servicies do not fail by themselves. Failure occurs in the context of an overall, national fiasco, caused by systemic problems that fall into three distinct but related categories:

✓ failure to anticipate the nature of and trends within the strategic environment; the character of the opponent; one's own will and resolve ; the impact of technology – be it disruptively new or employed in unexpected ways; and failure to anticipate the second and third-order effects of both action and inaction.

✓ failure to learn from experience-both one's own and other's. Selective reading of history is particularly pernicious here, as is mistaking "lessons recorded" with lessons actually learned.

✓ failure to adapt behaviors, concepts and institutional constructs to the ever changing domestic and international dynamic, as well as to evolving adversarial operational, technological and / or doctrinal innovations. Failure to validate pivotal assumptions and adjust accordingly falls in this category as well.

4. Instead of closing. Secret word: partnerships

The partnership, as a form of collaborative management and action, acquire a growing importance in the era of global security. In the world there are already several forms of partnership for security, all proved in various degrees its construction and utility.

Partnership's performance is based on several factors. The top two most important are partnership strategy and partnership collaboration. Partnership strategy envisages unified understanding of the security environment, making conception of action and monitors the results together. Partnership collaboration is based on identifying and defining together the goals and objectives of the action so to streamline as much operational plan-driven security.

Partnerships collaboration is a complex and dynamic procedural ensemble in the modern security plan, aimed at some special items, as follows:

✓ active and creative participation of the participants to achieve and develop common security;

✓ management contribution to developing concept, rules and actionable rules to operationalize forces and capabilities and permanent procedural standards;

✓ acquiring the ability to act jointly, based on unitary, rules set together and unanimously accepted by all participants to act superior managerial cohesion;

✓ willingness to be together all the problems and actions involved in modern security in different areas of existence or international missions and multinational;

✓ ability to work individually, but acting together or converging operational and capitalization shares lessons (lessons learned) in future preparations;

✓ achieving capabilities to operate/act together based on the plan and unique concept of modern features operations: network-based, combination, concentration and recovery effects, intelligence superiority.

Acknowledgement

This paper is made and published under the aegis of the Research Institute for Quality of Life, Romanian Academy as a part of programme co-funded by the European Union within the Operational Sectorial Programme for Human Resources Development through the project for Pluri and interdisciplinary in doctoral and post-doctoral programmes. Project Code: POSDRU/159/1.5/S/141086.

BIBLIOGRAPHY:

1. ALICE, Y. L. Lee, *Literacy and Competencies Required to Participate in Knowledge Societies*, in *WSIS+10: Overview and Analysis of WSIS Action Lines C3 Access to Knowledge and C9 Media*, accesed at http://www.wsis-community.org/ pg/ groupwiki/ owned/group:15325.
2. LANI Kass; PHILLIS J. London, Surprise, deception, denial and warning: strategic imperatives, 2012, Forign Policy Research Institute, winter 2013, orbis.
3. MAIOR, George Cristian, *Incertitudine gândire strategică şi relaţii internaţionale în secolul XXI*, Ed. RAO, Bucureşti 2009.
4. MAIOR, George Cristian, *State, reţele, companii şi indivizi: paradoxurile spaţiului cibernetic*, în volumul *7 teme fundamentale pentru România*, Ed. Rao, Bucureşti, 2014.
5. MAIOR, George Cristian, *Cuvânt – înainte*, în volumul *7 teme fundamentale pentru România*, Ed. Rao,Bucureşti, 2014.
6. MUREŞAN, Mircea; STĂNCILĂ, Lucian; ENACHE, Doru, *Trends in evolution of theory and practice of war*, Publishing U.N.Ap. "Carol I", Bucureşti, 2006.
7. ŢENU, Costică; STĂNCILĂ, Lucian, *Formele specifice conflictelor militare moderne*, Editura U.N.Ap., Bucureşti, 2005.
8. World Summit on the Information Society, *WSIS+10 Statement on the Implementation of WSIS Outcomes*, Geneva, june 2014.
9. World Summit on the Information Society, *WSIS+10 Vision for WSIS Beyond 2015*, Geneva, june 2014.
10. Aspen Institute Homeland Security Program 2014, section *The Global Threat Picture as the Defense Intelligence Agency Sees It*, 26 julie 2014, to be wached at *http://aspensecurityforum.org/media/live-video.*
11. ww.dni.gov/nic/NIC_2025_project.htm.
12. ww.dni.gov/nic/NIC_2030_project.htm.

PRINCIPLES AND METHODS ON MILITARY CONFLICT ANALYSIS

Ilie MELINTE
Major, PhD candidate in Military Sciences within "Carol I" National Defence University, Bucharest, Romania.
E-mail address: imelinte@hotmail.com

Abstract: *Military conflicts are both as part of or as an effect of crises, a permanent trait of human society, they are one of its elements and they are represented either as moments or as stages of its development. In most situations, both crises and military conflicts are obvious and they are shaped and determined both as outcomes of social, political, economic and especially military imbalances and of an entire faulty and inefficient chain of actions, activities or processes.*

We are not approaching the need to study the complex phenomenon of the military conflict merely because such need is obvious in the presence of conflict, but also because it leads to a better knowledge of conflict prevention and management and to the improvement of the scientific spectrum needed to develop the capabilities of the military structures that may be involved.

Keywords: *crises; military conflicts; war; analysis; perspectives.*

Introduction

The characteristics of each age, the level that society has reached and the types of relations that have been established, the level of conditioning and determinations are the elements that induce the dynamics of threats, dangers and challenges of social, economic, political and military security. Most of them can be encountered anyplace or anytime and they are easily identifiable to the purpose of analysing, of knowing and even of planning countervailing or appeasing actions. This is actually the daily activity of people and of organizations which allows them to function.

Unfortunately,"most threats, challenges or dangers within the human society come in an indefinite form, which renders them difficult to identify and thus impedes timely countervailing solutions."[1]The process of identification and analysis of these negative factors is burdensome also because they are variable and they develop based on equally concealed and hard-to-decipher patterns. Here are the characteristics of the threats, challenges and dangers that are not in any way linked to the origin or power of such factors:

- they envisage the entire human activity and generally everything that there is;
- they are dynamic, non-linear, unpredictable and, most of the times, complex;
- most of them are initiated or facilitated by the very structures or phenomena they will affect;
- they develop mutual conditioning based on random patterns;

[1] Viorel, BUȚA, Brigadier general (r) professor, PhD, *THE EVOLUTION OF NATO'S STRATEGIC CONCEPT – the continuity and flexibility of an alliance in the international security environment*, The Military Science Magazine, edited by the Military Science Department of the Academy of Romanian Scientists, No. 1 (22), Year XI, 2011, p.53.

- they efficiently rely on the weaknesses of the processes and of the systems they pursue;
- they generate and maintain new vulnerabilities.

The main effort is generally directed towards the protection of the structures and of the activities that are likely to be attacked; here is a condensed list of means to exercise such effort:

- creating within structures distinct security-dedicated forces, the purpose of which is to act and react to threats and dangers;
- creating and developing formations that are dedicated to the express internal security protection;
- creating specialized extrinsic (exterior) security structures, different from those presented above.

Nevertheless, security systems themselves are subject to threats and dangers, irrespective of their nature or value and they too are vulnerable, which triggers the need for a security concept for the systems that were created for security. But before designing tactics, strategies or policies for such concept, it is necessary to identify, analyse and assess the threats, dangers or challenges that aim expressly at such structures or actions.

1. Principles of military conflict analysis

The complex phenomenon of military conflict cannot be initiated randomly. Despite the fact that in this case too it is possible to carry out a thorough research in order to establish what is actually happening, just as well as in any other domain that requires the issuance and verification of hypotheses, military conflict analysis is not usually based on simulation, but on the research of existing things. The dynamics of the latest years iterates the fact that ”there have been too many and fairly complex conflicts, rendering simulations and experimentation unjustified.”[2] Moreover, although in this field too, similarly to other research fields, patterns may be designed and assessed, tested and experimented and then applied, reality provides the best source for the analysis of actual situations and yields excellent results.

Clearly, such situations cannot be chosen and analysed without using methods and principles. There aren't many principles applied to identifying and defining military conflicts and they are normally shaped by previous experience, by official documents, by identified analyses, reports, lessons, scientific studies and analyses and also by elements of the collective memory, which is what the human society has accumulated throughout history.

It is inferred from the literature of the field that there are two basic types of principles: the general type, valid for any kind of analysed situation, and the type that is specific of a certain activity or type of activity.

Also, before any activity, it is very important to identify and describe the principles that define and shape such activity and also to set up the rules that need to be followed. In doing so, it should be taken into consideration that principles are not very flexible and that in any case their field and extent are neither limited nor constant.

The following principles have been identified as necessary to abide by and apply in establishing the policies and strategies used in identifying the characteristics of military conflicts:[3]unity, flexibility, continuity, sufficiency, transparency, firmness, profoundness, self-correction.

---

[2] Răzvan, BUZATU, PhD, associated professor at National Defence College, Bucharest, *A new approach to analyze the current global system,* IMPACT STRATEGIC No. 1/2014, Publishing House of the „Carol I” National Defence University, 2014.

[3] ***, *CRISIS, CONFLICT, WAR Volume IV: Military and civilian-military systems used in crisis and conflict management*, Publishing House of the ”Carol I” National Defence University, Bucharest, 2007, p.236.

The principles described hereinabove are generally specific of the systematic and coherent research, which is a method of analysis of a phenomenon or process. Moreover, these are both analysis and synthesizing principles and also actual action and reaction principles. The above-described principles require an adequate, unbiased and responsible behaviour and they are applied especially by and within systems which are experiencing an imbalance caused by conflict and crisis. A clear understanding of the situation is the first step toward identifying a possible solution. If this first step is not taken, the result of applying a conflict management solution cannot raise to the expectations.

1.1. Unity

Unity (integrality) as a principle refers to the compact analysis of the processes and of the phenomena that determine, make up and influence the armed conflict throughout its duration and extent. The three main approaches to the principle of unity are: holistic, structuralist (analytical) and complex.

The first approach envisages the entity itself, with its specific attributes and its relating functions, with the elements that shape its individuality and its quality as a system.The holistic approach will nevertheless not suffice, as it provides a one-perspective knowledge of the system - integrality - and it omits the perspective that truly bestows upon it the force and substance that allows it to exist and evolve. The main shortcoming of using only this approach can metaphorically be described like this: ”losing the moon while counting the stars”.

The second approach has the purpose of offsetting this shortcoming. The structuralism (analytical, complementary) approach to the phenomena and processes that generate military conflicts brings out their aspectsregarding: internal realities, dynamism and evolution, networks, structural and functional links, centres of gravity or vital centres. The shortcoming of this approach seems to be the fact that it cannot identify and assess the relations between different systems, the gradual evolution of the phenomena that lead unequivocally to military conflicts.

The third approach, the complex one, is complementary to the first two approaches, which remain absolutely necessary for a detailed knowledge, as it can provide an opportune identification of the strong points and of the vulnerabilities of systems. Obviously, each case requires a definition of the complexity, which, in its turn, requires the acceptance of variables and of the probability of spontaneous evolutions with unknown and hard-to-control effects. Thus, rules and means of action must be approached flexibly and applied on each particular system of study.

1.2. Flexibility

The principle of flexibility is imposed by the multitude and diversity of activities, by the selection and assessment of the state and dynamics indicators, by the analysis and usage of results, by shaping certain decisions and also by the transition between each type of analysis. Military conflicts, in their totality, are complex and dynamic. Moreover, although conflicts generally go through the same phases and acquire approximately the same type of structure, each of them has a particular configuration, philosophy and physiognomy. The disastrous results or extremely serious consequences of both the process of analysis of military conflicts and of the process of direct exertion of force or of military intervention is caused especially by their inflexible approach.

Here are several defining elements of flexibility:

- accepting and acknowledging the chaotic character of the structures and phenomena of military conflicts;
- acquiring the physiognomy and philosophy of time;

- consenting to change and transformation;
- opportunely acknowledging and examining variations;
- concessive behaviour;
- creating and using the feedback principle.

Nevertheless, it must not be inferred that flexibility means renunciation, excess of tolerance or the purpose of establishing positive liaisons with all the actors participating in the conflict. It is necessary to accept the idea that this principle constitutes a main characteristic of the process of management of any military conflict, characteristic that is determined by the power to opportunely understand the variations of status and of dynamics, complex situations and moments and tensions.[4]

1.3. Continuity

This principle is considered necessary and compulsory at the same time. Determining the parameters of the complex phenomena that generate military conflicts is a difficult and burdensome activity. Normally, both conflicts and crises are consequences of either the evolution or the involution of systems and of processes that are characteristic of the human life, of communities, of organizations or of political, economic and especially military institutions of certain states, of international organizations or alliances. The timely identification of the moment in which certain systems and processes reach the verge of military conflict requires a series of comprehensive, coherent, long-term analyses.

The elements that provide continuity would be the following:[5]

- the existence of analysis systems and structures with permanent interconnections and a high degree of security;
- establishing coherent policies and strategies of military conflict management;
- establishing and using easily noticeable and assessable indicators;
- creating interoperable databases;
- finding and using efficient methods.

1.4. Sufficiency

In the process of establishing the characteristics of military conflicts, contrary to normality, it is noticed that the principle of *insufficiency* is habitually applied. It seems that analysts are never happy with what or with how much they have got. This principle of *insufficiency* leads to significant errors and mistakes is expert reporting and in decision making.

Insufficiency as a principle is of the justificatory type, based on the reasoning of the *lack of data* or of *it is not possible*.

As far as the principle of *sufficiency* is concerned, it consists of determining and establishing the minimum level of information necessary to sustain a decision or to initiate an action. To this effect, the first step is establishing the exact format of the decision, of the rules and of the limits of such action, so that the plan of data and information gathering is adapted to the requirements, realistic and efficient.

---

[4] Mihai, ZODIAN, PhD, assistant in scientific research, Centre for Defence and Security Strategic Studies, *The Waltzian neorealism and the policy pragmatism*, IMPACT STRATEGIC No. 4/2013, Publishing House of the „Carol I" National Defence University, 2013, p.65.

[5] ***, *CRISIS, CONFLICT, WAR Volume IV: Military and civilian-military systems used in crisis and conflict management*, Publishing House of the "Carol I" National Defence University, Bucharest, 2007, p.238.

1.5. Transparency

In the methods and processes used to determine the characteristics of military conflicts, this principle of transparency may be considered a borrowed one and consequently adopted.

The operations used to determine the characteristics of military conflicts are usually domain-specific, rigid, complicated and they do not raise much interest neither form the people assigned to plan and execute them nor from the public. Despite that, transparency is a necessary and useful principle for all parties involved, as it is indicative of involvement and attitude, namely of the degree of civilization.

The two coordinates of this principle are:[6]

- transparency of the information and of the image in the public space (manifests the spirit of respect, characteristic of the democratic civilization);
- transparency of the system and of processes (depending on the system, the transparency of meanings are attributes of complex dynamic systems).

1.6. Firmness

This principle is directly linked to flexibility. It is considered that firmness must begin where flexibility ends. But ”flexibility should not be mistaken for rigidity, because it means steadily abiding by and applying previously determined and accepted principles and it also means ruling out uncertainty and insecurity or adopting them under reasonable terms.”[7] Firmness in the activity of determining the characteristics of military conflicts and of their management concepts means:

- making use of all the legal instruments and of the available means with a view to acquiring a detailed knowledge of the process or of the phenomenon;
- staying within the boundaries of the law, of international law, of reality and of legitimacy;
- strictly abiding by the commitment rules and limits;
- protecting life, property, institutions, values and the environment;
- promoting and guaranteeing stability.

In order to accurately determine and evaluate the characteristics of military conflicts, which are various and complex, intelligence, realism, consistency, flexibility and a high degree of firmness are required.

1.7. Depth

Depth is based on the idea that processes and phenomena that are subject to analysis must be approached both completely and complexly, irrespective of the type of analysis (holistic, structural or complex). In other words, in order for the analysis to yield conclusive, consistent and profound results, it must be carried out both horizontally and vertically.

The horizontal analysis envisages mainly networks and the interconnections between them, the elements of conditioned probability, the identification of tangible results and the means of making connections, while the vertical analysis envisages time and space, with an emphasis on their fluctuations.

It is noticeable that the first type of analysis is linear, wholesome, covering the entire network, while the second type of analysis, which is specific of a superior level of approach, may be considered three-dimensional. These two types of analysis are complementary in that

---

[6] *Ibidem*, p.240.

[7] Teodor, FRUNZETI, General-lieutenant university professor PhD, *Content and dynamics of the current Revolution in Military Affairs*, IMPACT STRATEGIC No. 4/2013, Publishing House of the „Carol I” National Defence University, 2011, p. 10.

the horizontal one envisages the system status and the vertical one focuses on profound change.

From the experience of the process of military conflict management it can be inferred that these types of analysis are absolutely necessary, as they lead to a knowledge of reality, but nevertheless not sufficient, as their results are solely partial. Thus the need to add to these types of analysis another type, the complex analysis, which has a deeper profoundness.[8]

1.8. Self-correction

The endeavour to determine the characteristics of military conflicts is considered to have at least three interdependent aspects: divergent, convergent and unitary.[9]

Divergent activities have the advantage of having individuality and their own particular research techniques, and they are highly recommended for the analysis of military conflicts, which require a detailed search, using various forces, means and methods. As far as efficiency is concerned, it should not be considered a guarantee for a very strict coordination. The activity of determining the characteristics of military conflicts may be said to be unlimited and include divergent, convergent and unitary operations. The role of each type of operations is distinct and it must be taken into consideration by the efficient policies and strategies of military conflict management; this has been proven both through the experience of the participant forces in theatres of operations and through the unfolding of the latest open conflicts in the world.

Convergent activities usually focus on pre-established items and set up the coordination of efforts with a view to obtaining maximum effects in short periods of time and engaging a small amount of resources. These cooperative activities are carried out in the pre-conflict phases or immediately after the conflict outburst, when there isn't time to look for insignificant details.

Unitary (integrated) activities are highly consistent and extremely fast system activities used mainly during conflicts, which aim at determining the overall aspects of the conflict; they are absolutely necessary for underlying large operations. A great disadvantage is that details are omitted. An example are the bombings that NATO did in 1999 in Serbia, which were the application of a policy and strategy developed only on self-adjustment, with a poorly refined response system.

2. Methods of identifying the characteristics of an armed conflict

The methods used to identify the characteristics of an armed conflict and to establish the coordinates of the activities aimed at controlling it are first of all the instruments of sustained scientific research of such phenomena or processes. It is implied that only a thorough knowledge of the phenomena that are likely to initiate and develop military conflicts and of all their aspects can provide the solutions for adequate reactions or for the right approach.The main methods that have been identified to this effect would be: ongoing observation, surveillance, research, comparison, synthesising, assessment and prediction.

2.1. Ongoing observation

In reality, there are specialized structures that observe social, economic, political and especially military factors, phenomena and processes that are very well-organized and that are

[8] Teodor, FRUNZETI, General-lieutenant university professor PhD, *Conflict and negotiation in international relations – course*, Publishing House of the „Carol I" National Defence University, 2011, p.34.

[9] Petre, DUȚU, senior researcher, PhD, Centre for Defence and Security Strategic Studies within „Carol I" National Defence University, *Asymmetric or hybrid threats: conceptual boundaries to security and national defence background,* Publishing House of the „Carol I" National Defence University, Bucharest, 2013, p.24.

constantly in action in all the civilized states of the world. Moreover, well-known organizations such as UNO, OSCE, EU, NATO and also regional organizations, including the NGOs "have developed structures that are dedicated to observing the above-mentioned phenomena. For their observation activities, such organizations use personnel, sensors, specialized structures of various values (teams, commissions, committees) and also technical equipments with very high storage and analysis capacities. All these systems must be interconnected, and it is the human factor that provides them with the necessary fluency, consistency, discretion and efficiency".[10]As a means of identification of the characteristics of military conflicts, "the ongoing observation represents especially the formation and use of functional and compatible structures for detailed, specialized and sufficient gathering of data on the status and evolution of factors that can be perturbed by conflicts or that, alternatively, can trigger military conflicts."[11] The properties that the technical or human systems need to have may be summarized as follows:

- to ensure the permanence of the data-gathering process;
- to have operative data selection and storage capacities;
- to be permanently linked to databases;
- to function safely and be able to endure great fluctuations;
- to be flexible.

Observation should be not only permanent, but also methodical, in order to allow setting objectives and designing a coherent plan of selection of the data and informationnecessary both to determine the characteristics of the military conflict and to establish the efficient policies and strategies required to control its effects.

2.2. Surveillance

This method is integrated, in a general sense, in the observation method and is used during the final phase of the latter, the phase in which the data and information are arranged in a functional framework.Surveillance allows analysis factors to obtain at any time the data and information required to assess the status of the system or of the phenomenon under observation. Clearly, observation does not mean only data gathering, but also data preparation, transmission and access. Surveillance or monitoring is a complex process, which greatly influences the structuring and dynamics of the security environment and which entails:

- ongoing observation of a process or of a phenomenon, using all the available instruments, which should normally be legal;
- capturing and storing the entire amount of data and information;
- ensuring that such data and information can be opportunely accessed by those who have the right to do so.

As a method to determine the main characteristics of military conflicts, surveillance provides the coherent data and information support that allows specific measurement instruments to be established.This is extremely important, given that the characteristic structure of military conflicts is never a closed one, but always open and ever-changing.

[10] Viorel, BUȚA, Brigadier general (r) univ. professor PhD, *Interdependency between national interests and international interests*, in Strategic Impact no.2[43]/2012, p.59.

[11] Cătălin, TOMESCU, Brigadier general, Phd, *Participation in NATO operations - lessons and ways forward,* Strategic Colloquium No.4/2014, Centre for Defence and Security Strategic Studies within „Carol I" National Defence University, Publishing House of the „Carol I" National Defence University, 2014, p.2.

2.3. Research

This method, also known as *analysis*, means the detailed study of each component of a system. Efficient research is only possible when using complete and clear information.

Research may be initiated starting from the whole and ending with its components, from the total to its sequences, or from a part to the whole. In any case, research must include all components, the entire mechanism.

Sequential research may have, in any situation, convincing and noteworthy results. It is clear that this kind of research will never offer the integrated image required for important decisions, it will offer sequential images.Unfortunately,"in the history of military conflicts there is a fairly high number of cases of decisions that are based exclusively on the outcomes of sequential research."[12]The Israeli offensives of 2006 and of 2014 against the Hezbollah fractions of South Lebanon and of the Gaza Strip, which resulted in direct military attacks and thousands of civilian casualties, are telltale examples of decisions that were based on insufficient sequential research.

2.4. Comparison

One of the essential phases of the entire assessment process is comparison, because research cannot have a target unless it plans for clear results that can be compared, with the purpose of pinpointing the actual links between data, information and the outcome of their research.

Comparison is, nevertheless, a complex activity that requires experience, knowledge, ability, intelligence, capacity of assessment, sense of responsibility and even courage. Moreover, comparison also requires: clear criteria, qualitative and thorough data and information, very well established units of measurement or grids, intelligence and expertise in identifying special aspects and features.

2.5. Synthesising

Synthesising represents the essence and may be considered a product
of research and of comparison. This method is an excerpt, a consequence of research and of comparison, or a dynamic structuring resulting from the joining together of independent or of dependent components that may combine into a whole. In the activity of determining the characteristics of military conflicts, synthesis may have two formats: excerpt and construction.

Researching and comparing a great number of properties and determining the process or phenomenon that comprises them all or the properties that mirror directly the spirit of the analysed process or of the phenomenon yields the excerpt format. This action entails at least the following phases:[13]

1. identifying all the elements that need to be analysed (a, b, c, …,n);
2. determining and describing the characteristics of each element (x_1, x_2,…,x_n); $a\supset(x_1, x_3,\ldots, x_{n-7})$; $b\supset(x_2, x_4,\ldots, x_{n-6})$;…, $q\supset(x_5, x_7,\ldots, x_{n-1})$;$r\supset(x_1, x_2,\ldots, x_n)$;
3. identifying the element that comprises all the useful characteristics;
4. extracting the identified element.

The second format represents a construction resulting from the merger of elements and properties, a merger that allows the outcome to express a special structure, very important in the process of identification of the characteristics of military conflicts and of setting up a strategy to control and end them.

2.6. Assessment

---

[12]Francis, FUKUYAMA, *The End of History and the Last Human*, PaideiaPublishing House, Bucharest, 2008, p.14.

[13]***, *CRISIS, CONFLICT, WARVolume IV: Military and civilian-military systems used in crisis and conflict management*, Publishing House of the "Carol I" National Defence University, Bucharest, 2007, p.247

The above-described activities are followed by the phase of assessment of the identified or described results. The process of assessment or of evaluation means not only gathering and registering the established indicators and properties, but also a further effort to analyse and compare them.It should be taken into consideration that results do not always meet expectations; they will, nevertheless, be close to the truth or, in any case, a ground for debate. In other words, ”if the research and assessment of the characteristics and of the factors that make up or influence the state of conflict in the world were enough to reveal the characteristics, the structure and the value of military conflicts, this world would easily acquire universal harmony.”[14]Thus, the data discussed herein offers the real perspective on processes and phenomena and have a determining role in making decisions and in performing actions in the most adequate manner.

2.6. Prediction

Military conflicts do not appear and disappear completely; there is proof of the existence of a chain of causes both of networks and of effects.

It is a given fact that a military conflict does not appear out of the blue, as do meteorological phenomena: storms, rain, blizzard etc., neither does it appear spontaneously and then disappear suddenly. Moreover, ”military conflicts are structured and restructured closely, they have foregoing phases and especially consequences.”[15]For this reason, in order to determine the characteristics of military conflicts, it is essential to take into consideration the past, the present and the future. Each decision is preceded by a prediction and the quality of the decision depends on the quality of the prediction. A prediction that is likely to materialize provides conditions for making a decision that is very likely to provide a successful outcome.

Conclusions

The characteristics of military conflicts are mostly influenced both by the coordinates and by the restructuring standards of the new national and international environment of political, economic and military security, and by the dynamism and dialectics of the objectives underlying the enunciation, structuring, expression and imposition of the new policies of long-term economic development, of access to resources, markets or technologies and of the strategies used to solve the present and future threats, challenges and dangers that the world is facing.

Military conflicts have effects similar to the effects of crises: states, areas, regions or continents are affected when a major military conflict occurs.

The military conflicts of the beginning of this millennium have grown to be interrelated, interconnected and chaotic, of unpredictable intensity, extent, form and area, all aspects that are indicative of their high level of peril.

Similarly, the dynamics, fluctuation or unpredictability of crises surpass the same traits of the very processes that caused and nurtured them and become high-risk sources of instability and proneness to conflict. Crises occur as dramatic, long-term transformations; some of them take violent forms and even lead to wars, fostering mean policies and cultures that severely threaten the state of normality, legality and security.

Studying the complex phenomenon of military conflict using the principles and methods described hereinabove lays the foundation that military systems and actions, in the present state of facts caused by extended crises and developing military conflicts, need to

[14] Henry, KISSINGER, *Diplomacy*, All Publishing House, Bucharest, 2007, p.11.
[15]Mircea, MALIȚA, *Games on the World Stage. Conflicts, negotiations, diplomacy,* CH BeckPublishing House, Bucharest, 2007, p.24.

adapt their characteristics and capabilities, symmetrically and asymmetrically, in a balanced and imbalanced manner to the same extent. This has the purpose of preventing the involved structures from reacting and of causing them to act pre-emptively or preventively by taking and maintaining a political-military and strategic initiative.

Acknowledgement:

This work was possible with the financial support of the Sectoral Operational Programme for Human Resources Development 2007-2013, co-financed by the European Social Fund, under the project number POSDRU/159/1.5/S/138822 with the title ***"Transnational network of integrated management of intelligent doctoral and postdoctoral research in the fields of Military Science, Security and Intelligence, Public order and National Security – Continuous formation programme for elite researchers - "SmartSPODAS"."***

BIBLIOGRAPHY:

1. BUŢA, Viorel, Brigadier general (r) univ. professor, PhD, *EVOLUTION OF NATO'S STRATEGIC CONCEPT – the continuity and flexibility of an alliance in the international security environment,*The Military Science Magazine, edited by the Military Science Department of the Academy of Romanian Scientists, No. 1 (22), Year XI, 2011, p.53.
2. BUŢA, Viorel, Brigadier general (r) univ. professor, PhD, *Interdependency between national interests and international interests*, in Strategic Impact no. 2[43]/2012, p.59.
3. BUZATU, Răzvan, PhD, associated professor at National Defence College, Bucharest, *A new approach to analyze the current global system,* IMPACT STRATEGIC No. 1/2014, *http://cssas.unap.ro/ro/pdf_publicaŢii/is50.swf.* on 28.09.2014.
4. DUŢU, Petre, senior researcher, PhD, Centre for Defence and Security Strategic Studies within „Carol I" National Defence University, *Asymmetric or hybrid threats: conceptual boundaries to security and national defence background,* Publishing House of the „Carol I" National Defence University, Bucharest, 2013.
5. FRUNZETI, Teodor, General-lieutenant university professor PhD, *Conflict and negotiation in international relations – course*, Publishing House of the „Carol I" National Defence University, 2011
6. FRUNZETI, Teodor, General-lieutenant university professor, *National Power and Military Power*, in "WORLD 2011 - Political and Military (strategic and security studies)", Publishing House of the Technical and Editorial Centre of the Army, Bucharest, 2011.
7. FRUNZETI, Teodor, General-lieutenant university professor PhD, *Content and dynamics of the current Revolution in Military Affairs*, IMPACT STRATEGIC No. 4/2013, Publishing House of the „Carol I" National Defence University, 2013.
8. FUKUYAMA, Francis, *The End of History and the Last Human*, Paideia Publishing House, Bucharest, 2008.
9. KISSINGER, Henry, *Diplomacy*, All Publishing House, Bucharest, 2007.
10. MALIŢA, Mircea, *Games on the World Stage. Conflicts, negotiations, diplomacy,* CH BeckPublishing House, Bucharest, 2007.
11. MALIŢA, Mircea, *Between War and Peace*, C.H. Beck Publishing House, Bucharest, 2007.

12. TOMESCU, Cătălin, Brigadier general, PhD, *Participation in NATO operations - lessons and ways forward,* Strategic Colloquium No.4/2014, Centre for Defence and Security Strategic Studies within „Carol I" National Defence University on *http://cssas.unap.ro/ro/pdf_publicaŢii/cs04-14.pdf.* on 30.09.2014.
13. ZODIAN, Mihai, PhD, assistant in scientific research, Centre for Defence and Security Strategic Studies within „Carol I" National Defence University, *The Waltzian neorealism and the policy pragmatism*, IMPACT STRATEGIC No. 4/2013, Publishing House of the „Carol I" National Defence University, 2013;
14. ***, *CRISIS, CONFLICT, WAR Volume IV: Military and civilian-military systems used in crisis and conflict management. Dangers, Threats, Risks. Assessment and Testing Criteria and Methodologies*, Publishing House of the "Carol I" National Defence University, Bucharest, 2007.

APPLYING SCIENTIFIC METHODS IN INTELLIGENCE ANALYSIS

Ruxandra BULUC
PhD in humanities, Assistant Professor within "Carol I" National Defence University, Bucharest, Romania.
E-mail address: buluc.ruxandra@myunap.net

Abstract: *The method traditionally used in science and in intelligence analysis in order to obtain theories or hypotheses is induction. However, in time, it has exhibited its limitations and it has produced errors, as certain important pieces of information may be neglected or eliminated in order to obtain a coherent hypothesis. The scientific method, on the other hand, is not based on confirming a theory, but rather on whether or not it can be falsified. More precisely, a theory remains valid until such an event may appear that disconfirms it, falsifies it. Applied to intelligence, this method presupposes that the intelligence analyst does not collect information to confirm a hypothesis, but to falsify it because all hypotheses referring to possible international events are only suppositions which may at any time be proven wrong by new information. Therefore, intelligence analysis may be viewed as infinite criticism, meant to open new avenues for analysis and to validate the ones that are most resistant to falsification.*

Keywords*: the critical method, the falsifiability of theories, intelligence analysis.*

The scientific method has found its way into many domains of knowledge other than the one it was initially designed for, from social sciences to medicine, including intelligence analysis. It can now be encountered in several fields that deal with information on the one hand and with prognosis, predictions, anticipations on the other hand. However, it must not be wrongly understood that the scientific method has permeated these domains in the same form as it is employed in the natural sciences or in its entirety for that matter. These delineations require further clarification, as it is vital to comprehend the fact that there is a clear difference between the content of natural sciences and that of intelligence, which will be the scope of this article. When referring to the scientific method, we do not consider the content that it will be applied to, rather the logic, the algorithm that is to be employed when analyzing the various contents of different fields. In this respect, the scientific method belongs to the realm of meta-theories, which explore the inner workings of a system and not its constitutive parts individually.

Hence the challenges of transposing this method from natural sciences to intelligence analysis. The former deals with more static elements, with predictable patterns of behavior, while the latter focuses more on the study of human interaction, thinking and action which could be, and in most cases actually are, difficult to predict. It is this apparent unpredictability that prompts the need for a method to guide intelligence estimates, a method that could diminish the risk of error, which could have serious, life-altering consequences in such cases.

The analysis that we shall undertake in this article starts from an analysis of the shift in the nature of the scientific method from induction to critical thinking, and then it focuses on the ways this updated method could be applied to intelligence analysis, to what extent, which aspects and to what ends.

1. From induction to critical thinking

Traditionally, in science, induction, promoted by Francis Bacon, has been employed as the means of obtaining a theory starting from the data collected in nature or observed in a laboratory. However, this method has serious drawbacks as it does not and cannot guarantee that no other piece of information would come to light and contradict the theory. If theories are mere generalizations, it entails that they will forever be vulnerable, firstly because, by definition, generalization leaves out some details, bits and pieces of information in order to attain its final condensed form, and secondly because it is impossible for any scientist to verify that generalization in all its instantiations so that (s)he could make sure that there are no situations/circumstances which invalidate it. Simply because induction has functioned in the past (and this statement is, in itself, an example of generalization based on the history of science) it does not mean that it can suffice to guarantee the truth of any given theory. In fact, "experimental facts do not establish the ultimate truth of generalizations"[1], and, consequently, they cannot form the basis of any scientific theory.

As difficult, challenging, and possibly even counter-intuitive as replacing induction may appear at first sight, there is a solution put forth by Karl Popper who suggests that rather than trying to verify that a theory is true, based on the data collected, the scientist should, in fact, ascertain if it could not be refuted by the data collected. Popper argues that falsifiability is the best criterion of demarcation for scientific theories. In his words "[it is not required] of a scientific system that it shall be capable of being singled out, once and for all, in a positive sense; but [it is required] that its logical form shall be such that it can be singled out, by means of empirical tests, in a negative sense: *it must be possible for an empirical scientific system to be refuted by experience*."[2] It is important to notice that in the Popperian theory statements (be they basic, universal or existential) are considered out of the context of their production. It does not take into account the scientific community in which these statements are enunciated and focuses solely on the resulting theory itself.

Theories should be formulated so that they can be tested one against another by means of what he calls "inter-subjective testing"[3] This means that the basic statements of science can be tested by comparison but cannot be refuted unless the contradictory statements are regular and reproducible. (As we will show in the following section, this remark is of great use for intelligence analysis in which any statement that seems to refute a hypothesis has withstood, in its turn, the process of falsification.)

The difference between falsifiability and falsification is vital at this point. Individual statements are falsifiable, i.e. they can be contradicted by other statements, this is a trait they possess. This occurs only if those statements are reproducible, that is they are not unrepeatable occurrences. In this case the result is that either the theory does not apply in those cases or that it is not valid and thus the move has been made to the higher level where falsification (as a process) applies to theories.

Another aspect that Popper discusses and which is of interest for intelligence analysis refers to the probability of statements. He explains that "probability estimates are not falsifiable"[4] and they are not verifiable either since they deal with frequency and no matter how many experimental results may become available, one ca never fully establish with any certainty the exact frequency of an occurrence.

---

[1] Ben Israel, Isaac, (1989) „Philosophy and Methodology of Intelligence: The Logic of Estimate Process" in *Intelligence and National Security*, vol.4, no.4, Frank Cass. London, p. 665.
[2] Popper, K. (1959/2002). *The Logic of Scientific Discovery*, Routledge: London & New York, 3rd edition, p. 18.
[3] *Idem*, p. 25.
[4] *Idem*, p. 183.

However, Popper distinguishes between the probability of a hypothesis, of an event[5] and of a statement.[6] The probability of a statement may overlap the probability of an event but neither of these should be confused with the probability of a hypothesis. If an event is viewed as "a class of singular statements," then it can be transformed into a sequence of statements, and each statement can be assigned a truth frequency. When the class of statements is reduced to a single one, this can assume only one of two truth values: 0 or 1, according to probability logic. The truth frequency can be built back up to the probability of the event.

This method cannot be applied to the probability of hypotheses as they cannot be considered under probability logic as discussed above. Popper[7] asserts that if a hypothesis is defined as probable, then it cannot in any way be turned into a statement about the probability of events. Consequently, he puts forth the concept of corroboration[8], that is he suggests that instead of trying to ascertain the probability of a hypothesis, the scientist should try to assess "what tests, what trials, it has withstood; that is, we should try to assess how far it has been able to prove its fitness to survive by standing up to tests."[9] This way, if the hypothesis has been tested and withstood these tests, it can be declared corroborated and further used. This point is also relevant for intelligence analysis which deals solely with hypotheses and not with theories, and consequently, we would argue that it would be easier to corroborate a hypothesis than to falsify it, given its intrinsic probabilistic nature. However, the differences between the process of corroboration and that of falsification are essentially slim to none. The basic method is similar, in both cases the hypothesis or the theory, respectively, have to undergo testing to see if they are contradicted, the only difference consisting in the fact that once this process is completed a hypothesis still remains only probable.

All in all, the most important point that Popper makes with respect to scientific discovery and the one that is most applicable to intelligence analysis is that theories, once they have been enunciated, must not undergo a process of verification but one of falsification which proves more effective and also provides more secure results.

Thomas Kuhn[10] introduces another important point in the discussion of scientific discoveries, namely the way scientific revolutions come about. He begins by explaining that scientific problems are like puzzles and claims that the activity of normal science is to solve these problems within the set of rules given by the existing paradigm, that is within the accepted research tradition. Whenever a phenomenon appears that cannot be accounted for using the rules of the paradigm in place, then the first step available to the scientist is to extend that given paradigm, to refine it and to better it so that it may come to account for what at first seemed to be a counter-example. This brings Kuhn to the conclusion that "research under a paradigm must be a particularly effective way of inducing paradigm change."[11] In other words, the way to scientific discovery starts with the scientist becoming aware of an anomaly, meaning of a fact that seems to violate some part of the "paradigm-induced expectations."[12] This anomaly is examined and, in most cases, it leads to an adjustment of the theory so that it accommodates the anomaly. This is the way normal science operates. It is resistant to change, its first aim is to preserve the *status quo*, to refine the existing paradigm and the concepts it encompasses. This, in turn, leads to specialization, to the "restriction of a

[5] Popper defines an event as "a class of singular statements" (p.69) and adds that it denotes what may be typical or universal about an occurrence, or what can be described with the help of universal names (p. 65)
[6] Popper defines a statement as describing an individual occurrence (p. 65) by means of proper names.
[7] Popper, *op.cit*., p. 254.
[8] *Idem*, p. 248.
[9] *Idem*, p. 248.
[10] Kuhn, T. (1962/1996). *The Structure of Scientific Revolutions*, The University of Chicago Press: Chicago & London, 3rd edition.
[11] *Idem*, p. 52.
[12] *Idem*, p. 53.

scientist's vision"[13] and to a certain rigidity of science. However, this need not be considered a negative development, as, the more specialized the science becomes, the more sensitive it is to any anomalies, because anomalies can be detected only when the researchers' scientific background and apparatus are so refined that they know precisely what results are to be expected and thus they are able to ascertain that something has not gone according to plan. As Kuhn explains, "Anomaly appears only against the background provided by the paradigm. The more precise and far-reaching that paradigm is, the more sensitive an indicator it provides of anomaly and hence of an occasion for paradigm change."[14] It is vital for the development of science that paradigms exhibit this resistance to change because this means that researchers will not be easily sidetracked, led astray by irrelevant anomalies. Rather, by trying to understand how an anomaly came about using the means of the existing paradigm, they will in fact strengthen, reinforce and improve that paradigm in the process.

Crises appear in science only when, in the process of trying to explain an anomaly or a counter-example to a paradigm, the tools and conceptual apparatus of the existing paradigm prove inadequate. This is the moment scientific revolutions occur, this is the breaking point where a new paradigm emerges and replaces the old one. It is important to observe that a paradigm is rejected only once and when a suitable alternative has been found to take its place. "The decision to reject one paradigm is always simultaneously the decision to accept another, and the judgment leading to that decision involves the comparison of both paradigms with nature and with each other."[15] Thus, old paradigms play an important role the development of new ones, they are the background against which the new theory is tested and eventually validated. The scientists do not reject an existing paradigm just because one or several counter-instances have appeared, but rather because, after careful attempts to explain them using the paradigm at their disposal, they have discovered its shortcomings, they have failed to overcome them and they have devised another theory that does so.

Kuhn makes another relevant point: a paradigm is replaced by consensus in the scientific community. On this point, his theory diverges from Popper's who focuses solely on the theory and excludes the context of its production. However, especially with intelligence analysis in view, the community plays an essential role. The scientific revolution has a social component that cannot be overlooked. Simply because one scientist means to replace an existing theory, this does not lead to this change. Group support must be gained and this is, in our opinion, the social validation that any new theory must obtain, not only in science but in all fields of study.

Kuhn does not reject the concept of falsification proposed by Popper, but he refines it in light of his own theory of scientific revolutions. He explains that just because an anomaly has emerged, it does not automatically mean that the paradigm will be rejected. Falsification must then be doubled by verification, as the anomaly needs to withstand further tests that validate its claim and only after this process is completed can it truly lead to paradigm change.

Another philosopher of science whose contribution to the scientific method bears relevance for intelligence analysis is Paul Feyerabend[16]. He suggests a more comprehensive view of the scientific method which includes elements from both Popper and Kuhn as well as other aspects which have been left aside by theoreticians in this field. He believes that nothing should be excluded from the scientist's arsenal of investigation, including religion, metaphysics, or sense of humour so as not to restrict his imagination. Feyerabend's claim is that scientific breakthroughs appear when the researchers are not bound by restrictions, traditions, or standards. This liberal practice is, in his opinion, "both reasonable and

[13] *Idem*, p. 64.
[14] *Idem*, p. 65.
[15] *Idem*, p. 77.
[16] Feyerabend, P. (1993). *Against Method*, Verso, London.

absolutely necessary for the growth of knowledge,"[17] even more so for the domain of intelligence analysis as we will show in the next section. Theories developed within the framework of this liberal practice may at first appear to be incoherent, unreasonable, or nonsensical, but they are "an unavoidable precondition of clarity and empirical success."[18] In two words, the principle that Feyerabend puts forth for the development of novel scientific theories is anything goes, as long as it produces results.

In order for the scientist to understand the empirical content and to make the best of it, (s)he has to introduce as many views into his/her analysis as possible, i.e. to adopt a "pluralistic methodology."[19] Ideas must be compared to each other and the scientist must try to improve the ones that seem to fail at first glance, as incoherence and lack of clarity are only the precursors to clarity, structure and sound theories.

The reason why a scientist must not restrain his/her research only to one field but must embrace as many others as possible is that, in order to explain an event, one must be able to look at it from the outside. As Einstein said, a problem cannot be explained from the same level of consciousness that created it. External assumptions are needed in order to have an alternative that breaks the circle and constitutes the first step in the criticism of familiar concepts and procedures. "We must invent a new conceptual system that suspends, or clashes with, the most carefully established observational results, confounds the most plausible theoretical principles, and introduces perceptions that cannot form part of the existing perceptual world."[20] He calls this process counterinduction and it is the foundation of the method he proposes.

Counterinduction is the enemy of the consistency condition which Feyerabend believes should be disregarded because it eliminates a theory or hypothesis not on its faults, but rather because it disagrees with a previously adhered-to theory. Theories are changed when they disagree with facts, and Feyerabend's conclusion is that the discussion of incompatible facts leads to progress and, therefore, as many facts as possible, from as many sources as possible should be brought into the discussion to reveal their relevance, regardless of whether or not they prove contradictory or incoherent at first. Order arises out of chaos and it is all the stronger, the more chaotic are its origins.

In as far as the ways to ascertain which theories are valid are concerned, he shares Popper's view that one should always start with a theory and then see what facts can be brought into the discussion and what purpose they will serve. He does not discard falsification, but only postpones it to a later stage in the process, once the theory has started to form. In the initial stage, his only recommendation is open-mindedness. In this, his method is counterinductive as he also believes that induction is too limited to form the basis for relevant theories. However, this is where unavoidably the common elements with Popper ceases to exist. In Feyerabend's opinion, in order to obtain the maximal empirical content and develop the theory in all its complexity the scientist "will adopt a pluralistic methodology, he will compare theories with other theories rather than with 'experience', 'data', or 'facts', and he will try to improve rather than discard the views that appear to lose in the competition. For the alternatives, which he needs to keep the contest going, may be taken from the past as well. As a matter of fact, they may be taken from wherever one is able to find them - from ancient myths and modem prejudices; from the lucubration of experts and from the fantasies of cranks. The whole history of a subject is utilized in the attempt to improve its most recent and most 'advanced' stage."[21] His claim may appear unwarranted and overextended for the rigor

[17] *Idem*, p. 15.
[18] *Idem*, p. 18.
[19] *Idem*, p. 21.
[20] *Idem*, pp. 22-3.
[21] *Idem*, p. 33.

that scientific research requires at first glance. But its usefulness increases if one applies it to other fields such as intelligence analysis.

Feyerabend also believes, much like Popper but based on different arguments, that no theory can avoid being challenged. Existing theories appear to be timeless entities that have a degree of perfection and that are impervious to change. This is not actually the case. Science is complex and heterogeneous, it progresses in great leaps, but also in regresses, it incorporates both theories that have been neatly explained and "ancient and petrified forms of thought"[22] that can only be brought to light when challenged by new theories. This is the point where his theory joins Kuhn's to a certain extent. Kuhn argues that science is effervescent in the period before the crystallization of paradigms, when alternative concepts compete with one another and anything goes. Feyerabend adds the fact that the background movement towards previous theories on the verge of being refuted is a necessary first step to any progress as, in order to change a *status quo*, one must first bring it to light and explore its limitations. And this challenge may not come in the most rational and coherent of ways. On the contrary, Feyerabend argues that we need "these 'irrational means' in order to uphold what is nothing but a blind faith until we have found the auxiliary sciences, the facts, the arguments that tum the faith into sound 'knowledge'."[23] The history of science proves that ideas which seemed not to be in agreement with reason have survived, improved science and become an integral part of its progress. Although reason, coherence and logic are and become the desired outcome, they are not, in fact, the most efficient means of developing a theory. Deviations from the norm, apparent errors, sloppiness and chaos are preconditions of progress. As Kuhn also explains, turmoil and confusion are part of scientific revolutions and in the wake of the chaotic destruction of an old paradigm the new one is born. However, Kuhn views this process as sequential, while Feyerabend sees this chaos and the development of new theories as simultaneous and mutually inclusive.

2. The relevance of the scientific method for intelligence analysis

As different as these theories may appear upon initial examination, they actually share common points and they can be applied with some adjustments and in some respects to intelligence analysis. It should be made clear that the methods put forth by Popper, Kuhn and Feyerabend can be applied to intelligence analysis, but with a specification: they do not apply to scientific theories but to the hypotheses, statements and views that are the basic units of any intelligence report. These are not as accurate and decidable as the ones in the scientific realm, however, it is our contention that they can undergo similar processes of generation and verification/falsification. It is our claim that Kuhn's and Feyerabend's views are valid at the point of initial production of a hypothesis in intelligence analysis.

Firstly, Kuhn argues that an existing theory needs to be worked on and improved to accommodate new information that it may initially not be able to account for. This is the usual case in intelligence analysis, when the analyst in charge of a certain situation/country/conflict already has some views or hypotheses regarding the possible developments in that area. When new data becomes available that clashes with the views the analyst holds, the first step is to see to what extent those views could be modified to account for the apparently incongruous new data. If such a measure produces the desired results, then his/her hypothesis has been improved, the puzzle has been solved and the analysis continues.

If this, however, is not the case, and the new information cannot be incorporated into the existing hypothesis, then a period of chaos ensues that leads to the development of new hypotheses. At this point, Feyerabend's view of how such novel hypotheses are generated

[22] *Idem*, p. 107.
[23] *Idem*, p. 114.

becomes extremely useful. His rejection of boundaries, his appeal to liberal practice, his inclusion of all components of the human mind and its workings and products into the formulation of a theory leads to what intelligence analysis needs: as many open-minded and competing hypotheses as possible. They might at first appear ad-hoc, chaotic and unsupported by enough facts, but their generation is a very necessary starting point for any analysis and they should be allowed to float freely initially.

Diversity and unhindered imagination are to be promoted. All elements should be allowed to interact in this process of generation, not solely the ones that may most obviously bear relevance to the new data, but also components of previous hypotheses, imagination, religion, linguistic aspects, ideology, humour, etc. All these should be included and allowed to balance off one another in order to create as many hypotheses as possible. Moreover, the analysts should not feel flabbergasted if the resulting hypotheses appear contradictory or incoherent. In this initial, free flow of ideas, consistency and coherence are not relevant.

The community also bears great relevance for intelligence analysis, as it is only within a community that hypotheses can be generated and then undergo testing. Analysis in this field is not a singular or lone endeavour, a report passes through many hands before it is accepted and becomes a strategy.

Once they have been formulated, will these hypotheses come under scrutiny and undergo the process of falsification, which Popper proposes, to see if they are valid or not. It is also important to notice that this process of falsification is two-folded. Firstly, the data that become part of any hypothesis should be checked from as many sources as possible so that their validity is as secure as it could be. Secondly, the hypothesis itself undergoes the same process as it is compared against all available intelligence to see if any falsifies it. As Ben Israel[24] pointed out, the most efficient means of doing this, if several hypotheses are available, is to start with the boldest one, as it may probably be the most falsifiable. In the end, if more than one hypotheses remains standing, more data may need to be collected or the analyst may choose to present them all to the decision-makers.

Conclusions

The goal of this article has been to review philosophical theories regarding the scientific method so as to determine to what extent and which aspects could be translated to the field of intelligence analysis. Our contention is that Kuhn and Feyerabend's theories are applicable when a hypothesis is first generated, in the sense that, when facts are presented to analysts, they must decide whether they fit into the existing framework, or if the framework needs to be worked upon, adjusted to accommodate the new data. If both of these steps fail to produce a satisfying working hypothesis, then, in Kuhn's terms, the paradigm must be changed so that completely new hypotheses could be generated. At this point, Popper's concept of the falsifiability of theories becomes useful. Falsifiability helps ascertain which hypothesis is more plausible not by looking for information to confirm it, but rather for information that may invalidate it. This critical method, apart from producing sounder results, may also prove a more time-saving enterprise, as only one piece of information may falsify a hypothesis, while there is no amount of data that could ever fully confirm it.

The desired outcome of the combined scientific method we have proposed in this article is to ensure not only the solidity of hypotheses, but also to guarantee that their production is as unhindered as possible by preexisting biases, mindsets, preconceptions that might taint and the analysts' view and impede them from anticipating possible threats.

[24] Ben Israel, *op.cit*.

The strive for understanding, clarity and knowledge in all fields of human activity and the methods by which it is attained share common ground. Consequently, it is our belief that the scientific method, in an adapted form, can be transposed to the domain of intelligence analysis and yield more satisfactory results than induction ever could.

Acknowledgement:

This work was possible with the financial support of the Sectoral Operational Programme for Human Resources Development 2007-2013, co-financed by the European Social Fund, under the project number POSDRU/159/1.5/S/138822 with the title ***"Transnational network of integrated management of intelligent doctoral and postdoctoral research in the fields of Military Science, Security and Intelligence, Public order and National Security – Continuous formation programme for elite researchers - "SmartSPODAS"."***

BIBLIOGRAPHY:

1. BEN ISRAEL, Isaac, (1989) „Philosophy and Methodology of Intelligence: The Logic of Estimate Process" in *Intelligence and National Security*, vol.4, no.4, Frank Cass. London.
2. FEYERABEND, P. (1993). *Against Method*, Verso, London.
3. KUHN, T. (1962/1996). *The Structure of Scientific Revolutions*, The University of Chicago Press: Chicago & London, 3rd edition.
4. POPPER, K. (1959/2002). *The Logic of Scientific Discovery*, Routledge: London & New York, 3rd edition.

POSSIBLE NATIONAL APPROACHES IN THE CURRENT STRATEGIC ENVIRONMENT

Dorin-Marinel EPARU
Colonel, PhD, Associate Professor, Security and Defence Faculty,
"Carol I" National Defence University, Bucharest, Romania.

Abstract**:** *In accordance with the requirements of the Romanian National Defence Strategy, with requirements derived from the NATO Strategic Concept and the Lisbon Treaty rules on the basis of defence policy directions established by the Government Program 2013-2016, the strategic objective of defence policy is to generate the conditions for the increase of decision capacity and action of the military body, adapting the legal framework for the opportunities offered by the European community, the Euro-Atlantic and International Organizations empowering the national interests. Romanian Army, the essential national security element must be expressed in both meanings of approaching security environment: the national one - by taking the integrated management of the country's defence, in which state institutions complement and mutually support each other, and the international environment - by active contribution to defence obligations assumed by the Romanian state as a member of security and defence international and regional organizations.*

Keywords: *strategic environmental, defence policy, security, defence, national approaches.*

1. Military Implications of the Security Environment

We consider that the main challenges of the actual security environment and the predictions for the next ten years require a rethinking of the armed forces action, generally speaking from proactive perspective, able to build a new philosophy of command and control and to create new types of forces, capable of participation to the whole spectrum of operations[1] in the following conditions:

- Disappearance of classical framework of confrontation and appearance of fluid, digital, dynamic and 3D engagement space;
- Use of "noble" strategies, as effect of involvement of sophisticated weapons, incorporating intelligence and significantly reducing human imprecision;
- Promotion of an philosophy of dissimulation of aggressive actions in peaceful, seamless and subtle psychological influence, and of intoxication of communication means, simultaneous with engagement of strategic interest;
- Priority use of non-lethal weapons, and in limited situations, the lethal ones, only for strategic objectives;
- Emplacement of naval and air force strategic means, of mechanised and armoured from reserve, simultaneous creation of a lethal active component, made of small force packages, rapid deployable and with capabilities for counteraction of emergent asymmetric and hybrid threats.

The analysis of evolution of the security environment influences the armed forces, which promote actionable implication, most important being, in our opinion, the following:

[1] For details regarding the operations suitable for Romanian Armed Forces see Romanian Armed Forces Doctrine, Edition 2012, p. 45.

- Continuation of active accomplishment of Romania's security engagement, with accent on equitable sharing among allies and partners of specific duties and contributions in management of conflict situations and protection of energy resources;
- A new way of planning and execution of operations with accent on overwhelming approach of strategic environment and provocations on national security, including the non-traditional ones, such as energetic security;
- Transformation of Romanian Armed Forces and achievement of a modular joint operational force, and military capabilities super-specialised, prepared to face the future provocations;
- Optimization and rhythmic allocation of budgetary resources that will allow the flow of major national endowment programmes in areas like intelligence and research, technology acquisition and human resources.

For all these implications, the national forces shall have the ability to innovate during peace time and to adapt during crisis to the realities and opportunities of the hybrid engagement space, when fear for a war and the friction will denaturise, hide and influence the perception on engagement space reality. In addition, the armed forces will have to pose high availability, versatility, mobility and autonomy, interoperability and adapting capacity, increased reaction speed and information superiority, as well as increased capacity of self-sustaining of own forces.

2. National Military Actions Imposed by the Current and Future Geostrategic Environment

For the sake of direction of defence planning process, for the acquirement of strategic objective, in accordance with the level of ambition, the Defence White Book[2] establishes the following objectives of the defence policy:

1. Development of credible military capabilities;
2. Consolidation of strategic relevance within NATO and EU;
3. Development of bilateral and regional cooperation relations;
4. Support of public authorities in emergency situations, in order to assist the civil populace and consequences management.

2.1 National Military Actions Necessary for the Development of Credible Military Capabilities

In my opinion, for the development of credible military capabilities it should be implemented at least the military actions specified below, as follows:

- Prevention of surprise;
- Discouragement of military provocative actions;
- Defence of strategic objectives and host nation support infrastructure;
- Maintain and development of high reaction capacity, adapted to the level of threat in accordance with own strategic security environment;
- Cyber defence of the military command, control, communications, computer and information systems.

I consider that the *surprise prevention* should span over the surveillance and early warning during peace time and the assurance of strategic safety during pre-conflict.

I estimate that the *discouragement of military provocative actions* shall consider the strategic cover during the pre-conflict, and shall be based on the following success preconditions:

[2] 2013 Project, approved by National Supreme Defence Council

- Deployment of pro-active and efficient military diplomacy;
- Continuation of surveillance and early warning, of missions derived from combat and intervention service;
- Assurance of immediate reaction capacity for the transit to low-intensity military actions;
- Development of pro-active communication strategy specific to each provocative military action;
- Continuation of participation in the military missions, in accordance with assumed engagements.

From my point of view, the *defence of strategic objectives and support infrastructure of the host nation* suppose the transit to strategic defence during the conflict period and protection of strategically important objectives.

Maintenance and development of high reaction capacity, adapted to the level of threat, includes the assurance of required conditions necessary for the defeat of aggression, in allied context, during conflict, and the recovery of national potential after the conflict.

Finally, maybe the most actual subject of the global confrontation nowadays, the command, control, communication, computers and information military systems for protection, monitoring, analysis, detection, counteraction of aggressions and insurance of opportune response against the cyber threat of critical IT infrastructure shall be based on the following priorities:

- Development of strategic communication infrastructure, capable to provide the basic services for the command and control of the force structure;
- Opening of cyber defence and information security capabilities of military computer network.

2.2 National Military Actions Necessary for the Consolidation of Strategic Relevance within NATO and EU

The experience of the last ten, respectively seven years since the accession to the two organizations impose us to take into consideration the consolidation of the strategies relevance within NATO and EU, situation where we consider that the amplification of the national military action may be performed through the following measures:

- Active participation in NATO and EU operations and missions;
- Participation in the collective defence mechanisms, in accordance with Washington Treaty article 5, within the operational systems: NATO Integrated Air and Missile Defence System/ NATINAMDS, Allied Ground Surveillance/AGS, Air Command and Control System/ACCS and NATO Early Warning & Control/NAEW&C;
- Participation in common defence policy of the community air space inside of the mutual assistance and solidarity clause, in the eventuality of an armed attack;
- Development of the common NATO (the „Smart Defence" concept) and EU („Pooling & Sharing" initiative) capabilities;
- Implementation of NATO Connected Forces Initiative/CFI through participation in certification and validation multinational exercises, validation of lessons learned and application of common training standards for the development of interoperability level of forces.

In order to achieve *active participation in NATO and EU operations and missions*, we propose that national authorities offers the requested forces and capabilities, in accordance with the declared level of ambition, based on the following success preconditions:

- Continuation of ISAF[3] participation until the end of 2014;

[3] ISAF - International Security Assistance Force, Afghanistan.

- Implementation of NATO Training Mission Afghanistan/NTM-A lessons learned;
- Flexibility of the concept of usage of forces through the implementation of a planning system for deployable Task Force at brigade level, for action within the national territory and abroad;
- Participation in common training activities and multinational exercises in allied framework.

We consider that the pillar of Washington Treaty, *participation in collective defence system***,** requires the amplification of force packages established within the „Capability Targets" necessary for the alliance, based on the following success preconditions:

- Participation with staff and combat personnel within the NATO command structure and in theatre of operations;
- Participation in common training activities and multinational exercises in allied framework.

From the perspective of Lisbon Treaty, the *participation in common security and defence of communitarian space* within the mutual assistance clause in case of armed attack implies the offer to the EU of the NATO force package of the resources agreed at national level, based on the following success preconditions:

- Participation with staff personnel in the EU operational headquarters;
- Implementation, at national level, of the European procedures and standards for the crisis management;
- Participation in EU common training and multinational exercises.

For the participation in development of NATO common capabilities, in accordance with NATO and EU „Smart Defence" concept, and „Pooling & Sharing" initiative, we propose the following success preconditions:

- Multinational cooperation within „Smart Defence" initiative, on three specific directions: identification and hierarchy of critical capabilities requirements, promotion of extended defence cooperation, and development of NATO capabilities through innovative multinational approaches;
- Contribution to the development of critical alliance capabilities: AGS, NAEW&C, ACCS, Ballistic Missile Defence/BMD, Strategic Airlift Capability/SAC;
- Participation within the „Pooling & Sharing" initiative in order to cover the capabilities deficits in the following areas: operations medical support, counter improvised explosive devices (C-IED), air strategic lift fleet, logistic support, pilots' training and firing ranges;
- Contribution to the EU capabilities development programmes, under the European Defence Agency: Multinational Theatre Exploitation Laboratory Demonstrator / MNTELD, European Satellite Communication Procurement Cell/ESCPC/M, Combat Equipment for Dismounted Soldier/CEDS/M, European Air Transport Fleet/EATF, Diplomatic Clearances/DIC, MN Multinational Joint Headquarter/JHQ, Ulm, Germany.

From the performed analysis resulted that the *implementation of NATO interconnected force* may be produced through participation in force certification and validation multinational exercises, validation of lessons learned and increase of the forces interoperability level.

Obviously, the military actions necessary for the consolidation of strategic relevance has to include, mainly, the development of bilateral and regional cooperation relations, and secondly actions in support of public authorities (by populace assistance and natural disasters relief, extreme weather phenomena and technological accidents, in cooperation with specialised structures and participation with forces to the counterterrorist actions common exercises and training with the other forces of the national defence and public order system). My intention is to present these actions in a separate article, due to the utmost importance

within the national security system, but also due to the complexity of the defence policy domain. We consider that all these actions, effects and preconditions for success represents the minimum necessary for the accomplishment of efficient completion of the defence strategic objectives, in accordance with the national ambition level on the great „chess table" , where the regional and world actors has the imperative of own interests satisfaction, interests which may not coincide with the national ones.

Conclusions

In our opinion, Romania is a key factor in the regional geopolitical equation, and it may represent a trigger element in the decisional start on European level. Before the clicking of this event, Romania has to decide alone if the security warranties earned by the NATO and EU association are sufficient, or it has to express herself articulated in order to improve its strategic profile by fructification of the strategic partnership with Poland, for the benefit of the whole region stretching from Baltic Sea to Black Sea. We evaluate that, at global level, there is a tendency of growth of military component implication in missions which are not typical for militaries, based on NATO recommendation that the Romanian military structures to be able, in the future, to cope with global and regional risks and threats.

From the perspective of security assurances, we are convinced that any armed attack against NATO and respectively EU territory will generate a response in accordance with the Articles 5 and 6 of the Washington Treaty and/or the application of the mutual assistance clause in case of armed aggression, in accordance with article 28A7/ 42(7) of the Lisbon Treaty. Though, the Alliance and EU security interests may be affected by any emergent risks, such as terrorism, organised crime, migration as a result of armed conflicts, or restriction of energy sources.

We consider that in this fluid international environment, with threats difficult to predict, and limited resources available, it is necessary to involve a wide pragmatic scale of solutions for the articulation of military capabilities necessary for their countering, the most important being the following: the establishment of essential capabilities, the projection of functional force, able to sustain the own essential equipment, acquisition of equipments necessary for the acquiring of critical capabilities, acceleration of strategic endowment programmes, projection and development of capabilities for the cyber protection at the force structure level and participation at cyber defence at national and allied level.

Acknowledgement:

This paper has been financially supported within the project entitled ***"Horizon 2020 - Doctoral and Postdoctoral Studies: Promoting the National Interest through Excellence, Competitiveness and Responsibility in the Field of Romanian Fundamental and Applied Scientific Research",*** contract number POSDRU/159/1.5/S/140106. This project is co-financed by European Social Fund through Sectoral Operational Programme for Human Resources Development 2007-2013. **Investing in people!**

BIBLIOGRAPHY:

1. BĂHNĂREANU Cristian, PhD, *Securitatea energetică*, "Carol I" National Defence University Printing House, Bucureşti, 2008.
2. FRIEDMAN George, *The next 100 years: a forecast for the 21st century*, Ed. 2009.
3. TOFFLER Alvin, TOFFLER Heidi, *Wealth in Move*, Ed. 2006.
4. *** Romania Governmental Programme 2009-2012.

5. *** Defence White Book, Ed. 2013, project approved by National Supreme Defense Council.
6. *** Romanian National Defence Strategy, Ed. 2008.
7. *** Romanian Armed Forces Doctrine, Ed. 2012.
8. *** Romanian Energetic Strategy for 2007-2020, updated for 2011-2020.
9. *** Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation" Adopted by Heads of State and Government in Lisbon - Active Engagement, Modern Defence – 2010.
10. Titus Corlăţean, www.mediafax.ro/politic/duane-butcher-ne-angajam-sa-aparam-romania-12449685.
11. www.theguardian.com/world/2014/may/21/russia-30-year-400bn-gas-deal-china.
12. www.fonduri-ue.ro/res/filepicker_users/cd25a597fd-62/2014-2020/reuniuni-ciap/3_14.03.2013/9.%20Principalele%20repere%20ale%20dialogului%20cu%20reprezentantii%20CE%202014-2020.pdf.
13. http://ec.europa.eu/transport/themes/infrastructure/index_en.htm.
14. www.mdrt.ro/dezvoltare-regionala/programe-de-cooperare-teritoriala-europeana.
15. www.mae.ro.
16. http://ec.europa.eu/world/enp/pdf/com07_160_en.pdf.
17. http://ec.europa.eu/external_relations.

DEVELOPMENTS IN THE DISCURSIVE STRUCTURE OF DOCUMENTS CONCERNING ROMANIA'S NATIONAL SECURITY STRATEGY

Luminița CRĂCIUN
PhD, Lecturer, "Carol I" National Defence University, Bucharest, Romania.
E-mail address: craciunlum@gmail.com

Abstract: *Using the Alliance's new Strategic Concept approved by the NATO Summit in Washington in 1999 and the associated Action Plan on 23-24 April 1999 as references, this paper aims at highlighting the characteristic elements of the Romanian security related text-speech issued in 2001, before NATO integration, in comparison with the same security related text-speech issued in 2007 and the extent to which the Romanian security related text-speeches are correlated with that documents. The analysis is based on the comparative method and will be focused on identifying differences and similarities in the organization of the discourse structure, ways of encoding the linguistic of the concepts in the field of security, stylistic means used to express ideas related to national security precisely and coherently, capacity of the Romanian language to take over of the linguistic concepts in English in the field of security , and their adaptation to the Romanian specific language.*

Keywords: *national security strategy, discourse structure, linguistic concepts of security, comparative method, specific adaptation.*

Introduction

Romania's national security strategy is the framework document that stipulates the outlook of the state leadership on the defence and security of the state and of its citizens. The purpose of the strategy is to highlight the defence of the national interests and values, the promotion of the political, economic and social rights, the observance of the citizens' rights and human dignity, the identification of threats and risks, the avoiding of the crisis and conflict situations and of their consequences. Romania's joining the politico-military North Atlantic structures and integration in the European Union have imposed new rules as regards the elaboration of documents related to national security in which new roles, missions, stands and responsibilities are assumed.

We have set out from distinguishing the textual script from the wide range of definitions of the discourse (understood as enunciation, conversational activity, verbal interaction, etc) and we have attempted to analyse the texts included under the title *Strategia securităţii naţionale a României* - Romania's National Security Strategy - worked out and promoted by the Presidency of Romania. The analysis has targeted two documents, the former dated in 2001, the latter in 2007, which were initiated as a result of the provisos of the *Government Decision No.52* of August 12, 1998 on the planning of Romania's national defence[1], completed republished in Romania's *Monitorul Oficial,* Part I, No. 185 of April 28, 2000 on the grounds of Law No. 63 of 2000.

The above-mentioned Government decision, chapter 1, article 3 stipulates that the defining documents for the integrated outlook on the planning of national defence are:

[1] Text published in Monitorul Oficial no. 302 of August 18, 1998, official publication under the authority of the romanian government.

Strategia de securitate naţională, (The National Security Strategy), *Carta albă a Guvernului* (The Government White Charter), the strategies, plans and programs elaborated by the ministries and institutions with responsibilities in the field of defence, public order and national security[2].

Our starting point in the discourse/text analysis was a statement made by Dominique Maingueneau (1991), who states that discourse as the equivalent of the text is "a written enunciation, that is produced by institutions that strongly determine its enunciation, and it is confined to a strict interdiscourse that establishes its historic, social and intellectual, etc stakes"[3]. In our analysis we have taken into consideration the moment in which the respective documents were worked out (the landing mark was the joining of the NATO structures), as well as the ideological perspective offered by the presidency, as a state institution, the internal and international context of the period. We have used comparative analysis and quasi-qualitative analysis in order to pursue our objectives, and we have focused on the conceptual support that the discourse/text of the national security strategy offers for the drawing up of the documents specific to ministries in the field of defence, public order and national security, on the level of lexicalization of these concepts and on the linguistic influence exerted by assuming the NATO policies and doctrine after joining the organization

1. Text Organization

The National Security Strategy is a framework document drawn up by the highest institution of the Romanian state as part of the European interstate construct, which has to project the idea of force, power, capability, the message of responsibility for the partners involved in ensuring the security of the state. Therefore, in order to pursue this purpose, the document should be organized according to a logical structure, and be characterized by coherence and clarity in wording and form.

The National Security Strategy is centred on several themes around which the security field is built, consequently, the discourse/text of the security strategy is divided in chapters and subchapters The first document subjected to our analysis was drawn up in 2001, before Romania joined the North Atlantic Organization (2004) and the subtitle of the strategy is couched in a language that reminds of the language in use before 1989, during the communist era: "*the guarantee of the democracy and fundamental freedoms, permanent and sustainable economic and social development, joining NATO and integration in the European Union*". Excessive use of *and* as a connector results in the loss of the semantic value of the concepts and the dilution of the message. The main themes approached in the discourse/text of the analysed document can be relatively easily identified in the chapter titles.[4] For exemple: "*Romania's national security interests; The Objectives of the National Security Policy; The International Security environment; Risk Factors to National Security; Action Courses in the national Security Policy; The Resources of the Security Policy"*[5] .

The text is organized in an introduction and six chapters and begins with the message from Romania's President. We should remark the fact that there is no contents page to offer the reader a general image of the text or to help him quickly identify certain topics. His can

[2] The text of paragraph 3 was completed and republished in Monitorul Oficial no.525 of October 25,2000 , by adding a new document with effect on the national security state, namely the Governing Program (*Programul de guvernare)* and by changing the name of *The Government White Charter (Carta alba a Guvernului)* into *The Government Security and National Defense White Charter (Cartea albă a securităţii şi apărării naţionale a Guvernului).*

[3] Daniela ROVENŢA-FRUMUŞANI, – *Analiza discursului. Ipoteze şi ipostaze*, Tritonic Publishing House, 2005, p. 73

[4] *Strategia de securitate a României*, Bucureşti, 2001, p. 3.

[5] *Idem*, trad.

lead to the inference that the intention of the emitter was to create a sort of *halo* effect as regards the importance of the document for national security, rather than offer incentives towards concrete activities.

The subchapters have titles that are either complete sentences (for instance "*Europe is in Continual Change"/"Democracy is an Important Resource of the Internal Security Environment"*), or elliptic *(such as "An Active and versatile Organizational Framework"/"In the Social Field"/"The New Challenges"*) or even metaphorical *("Under the Umbrella of the International Climate")*.

The analysis of the second discourse/text - the Strategy of 2007 - indicates the use of repetition in the wording of the subtitle (*European Romania, Euro-Atlantic Romania/ România Europeană, România Euroatlantică)* in order to highlight the achievement of aspirations expressed in the post-December political documents. The concept of *democracy* is used as a determining lexeme to the nominal "*ţară*" (country), which makes reception closer to reality. The text of the 2007 Strategy also begins with the message of Romania's president, but this time the emitter is indicated merely by mentioning the information at the end of the message, and not in a title. The contents page reflects the organization of the test and includes the titles of the chapters , numbered with Roman figures and worded in a similar manner, that of elliptic statements. Here are some examples : „Chapter *IV. The Building of Romania's New European and Euro-Atlantic Identity; Chapter VII. Internal Security – A Systemic and Comprehensive Approach*" [6]

2. Content analysis

The internal and international contexts condition and influence the content of the speech on the strategy for national security, from both the conceptual viewpoint, and the semantic and pragmatic ones. Thus, the first speech we have examined, i.e. the 2001 Strategy, was designed before Romania joined NATO, shortly after the terrorist attack on 11 September, 2001. One can identify here concepts and types of wording, determined by the armed conflict that was unfolding in immediate neighbourhood of Romania, i.e. the former Yugoslav area, e.g. *identity crises, trends towards regionalization, fragmentation, marginalization, or isolation, development of good- neighbour relations, deterioration of traditional economic ties,* while terrorist organizations, which before September 2001 had not done anything that might have affected the Romanian state, were referred to using lexemes as "*entities", " phenomena",* or the collocation *" non-state actors"*.

The intention of joining NATO, and becoming integrated into the European structures, or the assumption of responsibilities, as a partner, is evidenced through the use of deictic wording, e.g. *the only ones capable of securing a status of independence* [7] (traded from Romanian: *singurele în măsură să-i garanteze un statut de independenţă),* with a "*natural significance",* i.e. *"a necessary process"*[8], or a *non-natural*[9] one, through the use of bold type[10], with the intention of providing the international organizations with the guarantees assumed by the Romanian state.

---

[6] *Strategia de securitate a României*, Bucureşti, 2007, p. 5, trad.
[7] *Strategia de securitate a României,* Bucureşti, 2001, p. 7.
[8] *Idem*, p. 8.
[9] According to H. P. Grice, *apud* A. Reboul; J. Moeschler, *Pragmatics of Discourse*, Editura Institutul European, 2010, p.139, the natural significance is not intentional, whereas the non- natural one „ implies intentionality, that of the locutor".
[10] Cap. 3.4: "The Romanian society is organized, and operates according to fundamental principles, values, and democratic liberties", *Strategia de securitate a României*, Bucureşti, 2001, p.15, cap.VI.
„ Achieving a climate of security, stability, and prosperity in the area of the Black Sea is a distinct course of action within this strategy", *Strategia de securitate a României*, Bucureşti, 2007,p. 32.

Despite the fact that the intention stated by the leaders of the state was that of joining the NATO structures, and becoming integrated into the European Union, the text itself does not impress through the clear wording of the commitment, but rather through a close resemblance to the so- called *wooden language*[11], which lacks the referential function, causing the reality to drift away, ultimately leading to the idea of the reality being dissimulated, or camouflaged. Thus, in the statement: "it is necessary [...] to adopt, as soon as possible, solutions that will lead to *genuine resumption* (traded from Romanian: *este necesară [...]* adoptarea neîntârziată a soluţiilor care permit o *relansare reală*"[12]) the referent, i.e. who or what to resume?, and in what way?, cannot be identified, and the qualifying determiner of the compound noun phrase has several semantic values e.g. *real*, as opposed to *fictional*, *dissimulated,* or *minimal*; "the polysemantism of the noun *foundation* in *providing security with a more solid, and effective foundation (*traded from Romanian: *tratarea securităţii pe baze mai solide şi mai eficiente"*[13]**)**, *;* the vagueness due to the use of polyphonic qualifying adjectives, i.e. *attractive, adequate,* the use of inversion, in order to give semantic emphasis to the determiner *mari (*traded from English: *big*), instead of the noun[14] - *fluxuri* (traded from English: trends) – "the economic resumption must be reinforced by creating an *attractive and stable business environment*, as well as by *adequately joining the big economic, financial, technological, and commercial trends"* [15] (traded from Romanian: *relansarea economică trebuie consolidată prin crearea unui mediu de afaceri atractiv şi stabil şi prin racordarea adecvată la marile fluxuri economico-financiare, tehnologice şi* comerciale"*).* Qualifying adjectives have as a result an idealistic view of reality, e.g. *serious social crises, new tensions, novelty of the strategy,* etc.

The abundance, in the speech, of verbal nominals, e.g. "*continuing the privatization*, *restructuring and modernization*, while focusing on the *dynamic growth* of the industrial fields*"* (traded from Romanian: *continuarea privatizării, restructurării şi modernizării, cu accent pe dinamizarea domeniilor industriale*[16]), as well as the use of the future tense result in a more abstract, and impersonal character of communication, and also in the strategy of using vagueness, which entails the avoidance of taking responsibilities, and making commitments:
The strategy acknowledges the necessity for achieving ways to stimulate national solidarity and civic responsibility…therefore, the efforts of the concerned institutions will mainly aim at:

- Promoting dialogue and social cohesion by involving the State, as a factor of balance, in countering the negative effects of the process of transition, as well as the developments of the market economy

(traded from Romanian: *Strategia stabileşte necesitatea realizării unor modalităţi de stimulare a solidarităţii naţionale şi responsabilităţii civice...ca urmare, eforturile instituţiilor cu atribuţii în domeniu vor avea în vedere:*

- Promovarea dialogului şi a coeziunii sociale prin implicarea statului, ca factor de echilibru, în contracararea efectelor negative ale procesului de tranziţie şi evoluţiilor economiei de piaţă…[17])

---

[11] Term suggested by Françoise Thom in her paper *La langue de bois*, 1987, referring to the highly clichéd political language of totalitarian regimes.
[12] *Strategia de securitate a României*, Bucureşti, 2001, p. 16.
[13] *Strategia de securitate a României*, Bucureşti, 2001, p. 16.
[14] „*The serious drawbacks of the wooden language must not be seen as a result of a clearcut project, of a genuine intention of manipulation. Many of them simply resulted from implementing the ideological premises".* Zafiu, Rodica, *Language and politics*, Editura Universităţii , Bucureşti, 2007, p. 32.
[15] *Strategia de securitate a României*, Bucureşti, 2001,p. 17.
[16] *Idem,* p. 23.
[17] *Ibidem,* p. 25.

In order to counter this impression, and render less grave the feeling of vagueness, binary syntactic structures made of items in partial synonimy, e.g. *the guarantee of rights and liberties, the development of the civil society and the middle class, the access to education and training* **(**traded from Romanian: *garantarea drepturilor şi libertăţilor, dezvoltarea societăţii civile şi a clasei de mijloc, acces la educaţie şi pregătire*) are combined with ternary structures, either simple or developed, which impart a sense of balance and precision, e.g. *continuing the privatization, restructuring, and modernization; the development of civic duties, social solidarity and intercultural dialogue continuarea* (traded from Romanian: *privatizării, restructurării şi modernizării; dezvoltarea civismului, a solidarităţii sociale şi a dialogului intercultural*).

Conciseness of the speech is achieved through rhetorical- stylistic features, such as enumeration, either simple, or developed, ellipsis, metaphor, e.g. *under the umbrella of the international atmosphere* (traded from Romanian: *sub umbrela climatului internaţional*), used within the corpus of the text, or even as chapter titles and subtitles.

The second discourse was drawn up after Romania joined NATO and started the integration process in the European Union - 2007, after two terrorist attempts were carried out in Europe, namely in Madrid in March 2004, and London, July 7 iulie 2005, and after armed conflicts have fundamentally altered the outlook on national security and defence in Europe and in the whole world. Consequently, the concepts related to the dangers threatening national security are expressed by liguistic structures and syntagms that highlight the complexity of phenomena, such as *international terrorist networks (*traded from Romanian: *reţele teroriste internaţionale*)*, terrorist groups (*traded from Romanian: *grupuri teroriste)*, or their intensity, such as *val de terrorism*/*wave of terrorism*. The text also includes lexicalizations of NATO concepts put forward at the 1999 NATO summit Washington, as, for example: *the indivisible character of global security, collective defence mechanism, common agenda of risks, security provider, connector of strategic importance,* which indicate the status of NATO member state. The influence of international documents can also be remarked in the use of various terms that have been borrowed or simply taken over, the use of compound words that have been joined together, (*reconstruction/reconstrucţie, postconflict/postconflict, resolidarization/rezolidarizare*) or linked (*contracarare pro-activă/pro-active counteracting*). Excessive borrowing also resulted in the emergence of barbarisms such as *sustenabil*, which attempts to replace an overused lexeme in the communist period : *sustained efforts (***trad.** *eforturi susţinute)***.**

The discourse/text of the Strategy worked out in 2007 is characterized by ample compound and complex sentences, the elaborate use of genitival nominals in order to explain in detail the strategic concepts that Romania had adopted once joining NATO and started the integration process in the European Union Here is an example: "*Romania will increase her participation and the promotion of democracy, security, peace, and prosperity in her good neighbouring policies and the operations for the management of regional crises and the securization of energetic and commercial flows"(* traded from Romanian: *"România îşi va spori participarea şi promovarea democraţiei, securităţii, păcii şi prosperităţii în cadrul politicilor de vecinătate şi la operaţiunile de gestionare a crizelor regionale şi de securizare a fluxurilor energetice şi comerciale"*[18]*.)*

The use of temporal deictics (marks for past, present and future), contributes to better anchoring the discourse in reality and offers a comparative perspective on the state of security of the country. This contributes to building the trust of the public in the institutions that have responsibilities in the field of security. The lexicalization of concepts in this field is based on the qualifying determinant "*strategic": strategic partnership, strategic interest, strategic*

[18] *Strategia de securitate naţională a României*, 2007, p. 28.

infrastructure, strategic roles, strategic identity, strategic importance, strategic options, strategic area (trad. *parteneriat strategic, interes strategic, infrastructură strategică/, roluri strategice, identitate strategică, importanţă strategică, opţiuni strategice, areal strategic*) or of the prepositional determinat *"de securitate"("security" used as an attribute) in constructions such as (furnizor de securitate/ security provider, actor de securitate/ security actor, paradigmă de securitate/ security paradigm).*

The rhetorical and stylistic devices that have been identified in the text contribute on the one hand to the economy of language and to semantic conciseness (ellipsis, enumeration, etc), and on the other they put the semantic stress on qualifying adjectives. There are examples of inversion –" *new risks and threats, the new security environment, better national cooperation (*traded from Romanian: *noi riscuri şi ameninţări, noul mediu de securitate, mai bună coordonare naţională) and* of metaphoric inversion - *the new opportunity window (*traded from Romanian: *noua fereastră de oportunitate*). The multiple adjective used according to the "rule of the three", as in "*state stabile, democratice şi prospere/ stable, democratic and properous states"* has the role of persuading and convincing.

Conclusions

The linguistic demarche that has been made to compare and contrast the two discourses of Romania's defence strategies has pointed to the evolution in the structuring, organization, and the elaboration of the written message. While the text of the 2001 Strategy is characterized be vagueness and imprecision in formulation, due to the use of linguistic clichés and lack of reference, the second discourse, that of the Strategy worked out in 2007, stands out due to the adequate use of terms specific to the field, connection to NATO documents, the minute and careful wording of ideas, clarity, conciseness, and coherence. This latter form of the document can be a real source of information for the elaboration of strategies by the national institutions involved in the field of security, provided that is updated with information and concepts related to security strategies put forward by the North Atlantic Alliance and the European institutions.

Acknowledgement:

This work was possible with the financial support of the Sectoral Operational Programme for Human Resources Development 2007-2013, co-financed by the European Social Fund, under the project number POSDRU/159/1.5/S/138822 with the title ***"Transnational network of integrated management of intelligent doctoral and postdoctoral research in the fields of Military Science, Security and Intelligence, Public order and National Security – Continuous formation programme for elite researchers - "SmartSPODAS"."***

BIBLIOGRAPHY:

Documents :

1. Preşedinţia României - *Strategia de securitate a României*, Bucureşti, 2001.
2. Președinţia României - *Strategia de securitate a României*, București, 2007.

Books in the field:

3. MAINGUENEAU, Dominique – *Analiza textelor de comunicare*, Editura Institutul European, Iași, 2007.
4. REBOUL, A.; MOESCHLER, J. – *Pragmatica discursului*, Editura Institutul European, Iași, 2010.
5. ROVENŢA-FRUMUŞANI, Daniela – *Analiza discursului. Ipoteze și ipostaze*, Editura Tritonic, București, 2005.
6. ZAFIU, Rodica – *Limbaj și politică*, Editura Universităţii, București, 2007.

INSTITUTIONAL COMMUNICATION STRATEGY DURING CRISIS: SOCIAL MEDIA – OPPORTUNITIES AND CHALLENGES CASE STUDY – GREAT BRITAIN STRATEGY

Gherghina OLARU
PhD candidate in Intelligence and National Security with "Mihai Viteazul"
National Intelligence Academy, Bucharest, Romania.
E-mail address: olarudn@yahoo.com

Abstract: *Known as an important tool for increasing transparency and responsibility to citizens in the digital era, the efficiency of an institutional communication strategy depends on the capacity to adapt to various means of message dissemination.*

Without mitigating the importance of traditional media, as television or newspapers, in current paper we shall theorize that the usage of social media has become a "must" in times of crisis, real time updating making easier for people to be informed and prepared, to react and counter react to biases.

For an institution, getting social media into communication strategy means new training programs for the personnel, in order to manage the specific tools and to expand virtual connections, with the goal of achieving higher credibility.

We shall get a closer look to the way Great Britain approached this area, keeping in mind that British authorities have already released a complex virtual communication strategy.

Keywords: *social media, communication, strategy, crisis, interaction, mobilization.*

Introduction

If we were to define "social media", its meanings would revolve around social interaction during which people virtually create, share or exchange data and ideas. Amid this interaction's features would prevail the large number of actors, from various places, the velocity of getting the message to the target and the constant attainability of information.

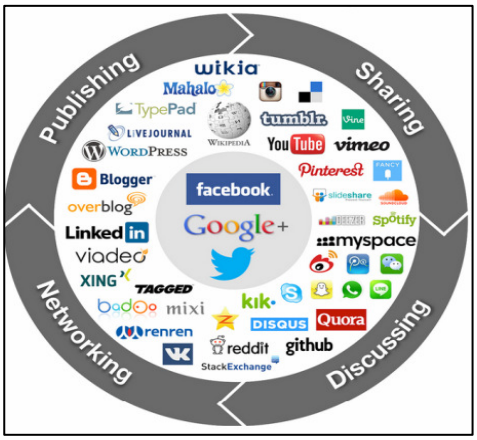


Figure no.1. Social Media Landscape
Source: www.fredcavazza.net

During the last two decades, virtual social networks have seen one of the most dramatic evolutions. Nowadays, over 1.6 billion people are using them. Such an uprising has generated a great speed of spreading the information. Statistics have shown that, every minute, 320.000 tweets and 120 hours of video are shared globally[1]. By usage, social networks can be sort into: blogs (Wordpress, LiveJournal), audio-video sharing (Pinterest, Youtube, MySpace), sharing ideas (Facebook, Twitter, Google+) or business connections (LinkedIn)[2].

Amid these, the most accessed are Facebook, Twitter and Google+, getting significant rises every year, thanks to complex sets of tools for publishing, sharing and posting.

Facebook is the most popular and broad social network, the using trend being greater and greater. Nowadays, Facebook has over 1.317 billion users, over 170 millions more than last year, out of which 1.01 billion use mobile terminals as the main way of connecting[3].

Twitter is the main competitor, although the users' number is significantly lower – 550 million users. Yet, the network, used primarily by public figures – journalists, politicians, artists – reported a 44 growth rate during 2010 and 2014. A close enough growth rate was reported by Google+ - 33, with over 1 billion users.

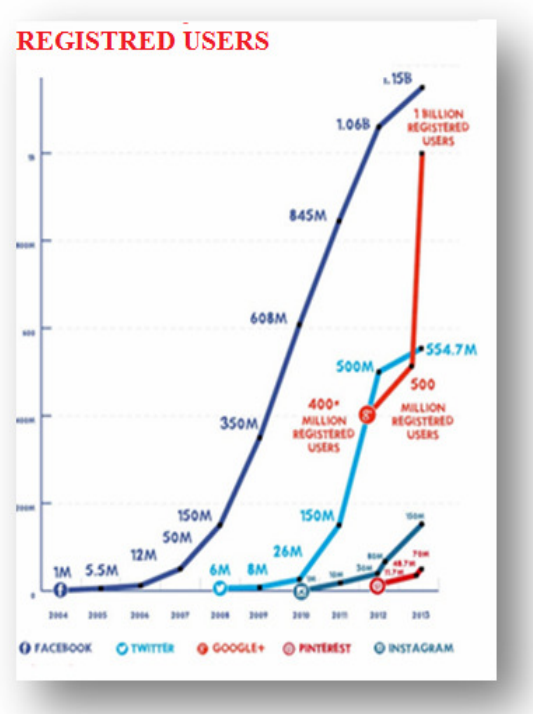


Figure no.2. Users
Source: adapting www.mediabistro.com

[1]Shea BENNETT, *Twitter, Facebook, Youtube, Google, Instagram, Snapchat – The Internet In Real Time [INFOGRAPHIC]*, 26.05.2014, available to www.mediabistro.com/alltwitter/internet-real-time_b57420, accessed in September 8, 2014.
[2]*Frederic CAVAZZA, Social Media Landscape 2014, 22.05.2014, available at www.fredcavazza.net/2014/05/22/social-media-landscape-2014, accessed at 06.09.2014.*
[3] David COHEN, *2Q EARNINGS: Facebook Has 1.32B MAUs, 1.07B Mobile MAUs, 399 M Mobile-Only MAUs,* 26.07.2014, available to allfacebook.com/2q-2014-earnings_b133449, accessed at September 7, 2014.

1. Social-media and Institutional Communication

Social media specially featured communication has drawn in the interest of institutional community, which is increasing the message disseminating through these channels, inclusively in times of crisis. Governments have grasped the utility of the new channels from the immediateness of communication, which allows the user to update the targeted public in almost any given situation, to constantly get and give away information from any given place on the globe, to speaking to the other users, no matter of time and space constrains.

It is obvious that the new form of communication in crisis has generated a new set of rules or, where applied, an adaptation of classical institutional communication settings.

Unlike classical forms of communication, social media is a bidirectional channel between government agencies and the public, allowing community members to disseminate data in real time[4], including details and links to useful information, to a large number of people, in order to reduce panic. And, last but not least, the costs are reduced[5].

1.1 Setting up the communication plan

Switching over to a greater use of social media communication by the government agencies in a crisis situation not only impacts the networking and the communication with the citizen, but also results in changes regarding practices and organizational culture, as well as alterations in the way of organizing and political hierarchies.

The decision of using the social media in the specific communication throughout a crisis context must be underlined by a preemptive plan. The latter should contain a list of the most probable crises and criticisms that may occur together with a list of possible reactions.

Thereby, objectives can be easily set as well as defining the limits of what is considered to be a possible threat in the social media area. Throughout this endeavour, we have to bear in mind that a identifiable crisis in the social media has the following characteristics: it is asymmetrical, meaning that the government knows less that the targeted public regarding the occurring situation; it is an important change towards the general approved norm and holds a great real-impact potential on the government institutions' activities[6].

Furthermore, such plan must imply software acquisition and also a web domain, in order to identify in time the crises that may break out in the virtual environment, but also for the communication of the team with the outside. A RSS system will also be created on the website so that the personnel can follow it. It is necessary that the personal virtual spaces (such as Twitter/Facebook accounts, blogs, etc.) are being connected together so that the communication could be realized using all sort of formats (pictures, videos, etc.).

A list of the most powerful followers of the official channels may prove to be very useful as these people may have an important role in the citizens' mobilization in a crisis situation.

---

[4] Gerald LEWIS, Gitanji LAAD, *Role of Social Media in Crisis Communication,* January 2014, available at http://www.geraldlewis.com/publications/Role_of_Social_Media_in_Crisis_Communication_Jan_2012_Gitanjali_Laad.pdf, accessed at September 7, 2014.

[5] Gerald LEWIS, Gitanji LAAD, *Role of Social Media in Crisis Communication,* January 2014, available at http://www.geraldlewis.com/publications/Role_of_Social_Media_in_Crisis_Communication_Jan_2012_Gitanjali_Laad.pdf, accessed at September 7, 2014.

[6] Adele Halsall, *The 5 Step Guide To Using Social Media in Crisis Management, 26.06.2014*, available www.jeffbullas.com/2014/06/26/a-5-step-guide-to-using-social-media-in-crisis-management, accessed at September 7, 2014.

The practice has proven that in order to have a successful public policy concerning the use of social media throughout a crisis situation, it must rely on a citizens' preceding preparation. The citizens must be informed in terms of the social media sources used by the Government, rules of usage, explanations regarding the organization's objectives when the social media is used as well as instructions of how they should act[7].

1.2 Great Britain – A Functional Model

Being aware of the amplitude of the social media phenomenon, and equally of its conveniences and challenges, some governments have framed their communication strategies to this new environment, a comprehensive model being suited by Great Britain.

The fundamental premise has been that, in times of crisis, communication is essential in Government strategy. As such, the officials' actions focus on preventing crisis form happening, from amplifying, as well as on providing a proper response when the crisis is not to be avoided.

The 2014-2015 British Government Communication Strategy is comprised of several public campaigns, for which social networks would be used: promoting the country brand, competitive economy and social conformity.

Until now, government analyses have shown that tactical communication is good, but strategic communication is weak. So, strategic planning, hiring policies, professional management and digital communication have been discussed. There have been over 2000 trainings, 95 mentoring partnerships and an internal evaluation network has been developed.

The practicability and efficiency of British model are based on the fact that the Government has understood that, if Internet and social sites go political, so must do the institutions, the main challenges being the targeted public, new trends in communication and personnel training.

At the beginning of 2014, a new Government structure was created – the Governmental Communication Service/ GSC, for providing the support for developing Government-population communication.

It has become essential to British Government to constantly adapt to an environment in which social media is more and more persuasive, in which insurgents and terrorists understood the conveniences of strategic communication and made it the central point of their campaigns. As a result, an essential aspect of the strategy is the audience, which may consist of citizens of every nation.

Great Britain is also aware that social media came with new forms of communication and social involvement, as "citizen journalism", "participant web", "peer to peer media", "social networking", "video-sharing", "live streaming", "virtual worlds", "web activism", all of that being out of the Government control, in a conventional way of putting it.

Nowadays, events are disseminated in real time by Facebook and Twitter. Given the context, any delay in Government reacting may be negatively used.

An important stage in the implementation of the new vision is to prepare the team, and that is the reason why the strategy for 2014-2015 is aimed at increasing digital capabilities at employee level.

---

[7] Cécile WENDLING, Jack RADISCH, Stephane *JACOBZONE, The Use of Social Media in Risk and Crisis Communication,* in OECD Working Papers on Public Governance no 25, OECD Publishing, 2013 available at http://www.pavillon-orange.org/blog/wp-content/uploads/2013/12/The-Use-of-Social-Media-in-Risk-and-Crisis-Communication.pdf, accessed at September 11, 2014.

To this end, the Government Service for Communication has assumed as one of their priorities making compulsory for officials to have digital communication skills and continuing professional development program for all communicators of the Government.

In one of the first stages we identified the training needs of staff in the middle-management tier and the management and modi operandi of the respective departments were restructured.

At the Government level, a team was created: it will coordinate the implementation of public communication strategy, including the structure of centers of excellence.

Furthermore, GSC plans to initiate in central government departments and certain local governments, a pilot staff recruitment program.

The strategy requires that each department has a team of leaders with the responsibility of coordinating all activities in the online environment, whose actions will be coordinated with those of the similar structure in the cabinet of the Prime Minister.

New functions have been established, staffed with specialists in communication and IT skills, with the tasks to supervise the online activities of other employees.

In this way, a network of coordinators is created, structured on several levels with different responsibilities, but with interrelated activities that can deliver at any time, a "rapid reaction force" in crisis.[8]

2. Communication management

Any advantage of a form of communication can turn quickly, especially in crisis situations, in its reversal, with potentially serious consequences on the state of security.

Expanding social media has increased the risk further by spreading bidirectional communication: posts not only by the authorities but also the users.

Adele Halsall, researcher of social media trends, theorized the fundamental aspects that institutions must take into account when they are in a position to manage a crisis that became public[9]. From her perspective, the most important factors are reaction speed, the control of messages, creating a tool for gathering responses, highlighting the actions that were taken and balanced reactions.

[8] *Government Coomunication Plan 2014/15", disponibil la https://gcn.civilservice.gov.uk/wp-content/uploads/2014/05/Government-Communications-Plan_201415_webSmll.pdf, accessed at 09.09.2014.*

[9] Adele HALSALL*, „The 5 Step Guide To Using Social Media in Crisis Management", 26.06.2014*, available at www.jeffbullas.com/2014/06/26/a-5-step-guide-to-using-social-media-in-crisis-management, accessed at September 7, 2014.

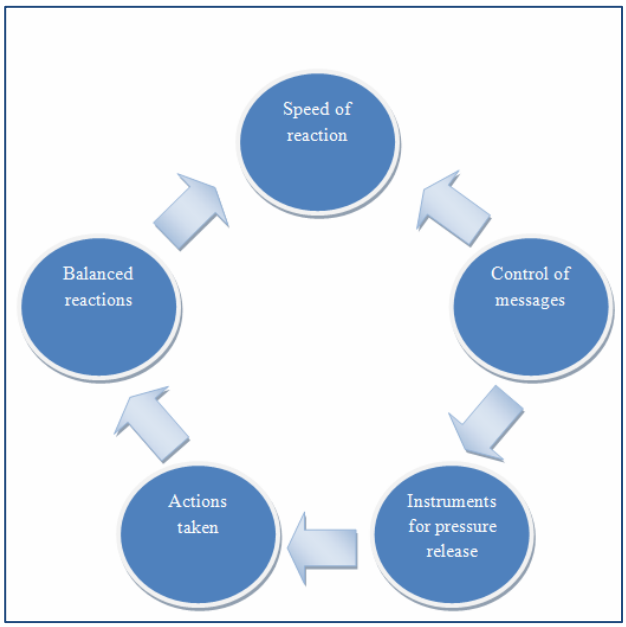


Figure no. 3. Communication in crisis situations

2.1 When and what do we communicate through social media

The immediate initiation of communication with the target audience sends a signal of attention to the community: it demonstrates that the authorities are present and willing to resolve the situation and contributes to winning the trust of the citizens.

According to experts, the maximum estimated time for a rapid reaction is 4 hours, and the first response of the team that managing the crisis should reflect that it knows that something happened, even if the institution does not have any information.

Even if there is no explanation (for now) of the crisis situation, it is essential that the target audience has at its disposal ways to respond effectively to the situation. From this point of view, the message should include a brief description of the situation and actions that are performed to solve the crisis and also, instructions to the public. It is essential that the construction and size of the message to take into account the characteristics of each communication channel and more than that, the accessibility from different devices (laptop, tablet to mobile phones).

Figure no.4. Official message content

The reaction speed will also be proof of the transparency in actions and will allow the issuer of the message to provide the public with ways of reacting. Equally as important is the frequency of updates. Throughout the course of the crisis, official communications should occur at every hour, even if the message does not contain new elements.

It is important for institutions to have their own channels of communication on all types of social media and be ready to post any kind of information (text, video, etc.)

anytime from anywhere on the globe on topics related to the crisis and chose to use the advantages of each social media category.

Facebook and Myspace as platforms for real-time communications can help improve coordination between volunteers and authorities. Content sharing platforms such as YouTube and Flickr can help situational awareness by identifying pictures or videos of how the crisis evolves in real time. Wikis and podcasts allow participants to ask questions and receive answers from different users. Blogging and micro-blogging tools like Twitter also can be used to share data in real time and communicate recommendations and warnings very quickly[10].

Responses should be offered in order of appearance of the posts signaling the crisis. For example, if the first such post appeared on "Facebook", the first official reaction should be posted on Facebook as well. Even if the institution is not present on one of the social networking platforms, it must be prepared to respond, by constantly monitoring posts that may be related to the crisis.

2.2. The control of the messages and the building of the reactions

Message control is essential, given that, in times of crisis, social media is usually the first place where users post their comments and inform themselves about an event. To obtain control, governmental agencies must be the primary source of credible information and, equally as important, they need to remain on this position until the end of the crisis.

Preferably, the places where users search information are to be limited. Otherwise there is a risk that information spreads, is erroneously interpreted and focus on the subject can be lost.

To this end, one can choose a platform on which to post all the information and can use other platforms to redirect traffic to the primary source.

Creating a site dedicated to the crisis situation can also be an option and all information relating to developments will be found therein. This strategy enables us to provide answers to the target audience by using a simple link instead of an elaborated text. In this way, you can avoid misinterpretations.

From the perspective of the specialists, this site should include: recognition that there is a crisis; details of how and where it happened, photos and videos, if available; how the institution has learned about the crisis situation; who was alerted, when and how; actions were initiated to resolve the situation; actual or potential effects; measures taken to prevent a similar crisis; contacts for use by the target audience.

It is recommended for institutions to create space on their social-media channels (the "comments" on the site dedicated to the crisis, the Facebook page of the institution, blog or forum on the website) where the target audience might express their opinions and frustrations accumulated during the crisis.

In the absence of such an instrument, it is possible for the public to turn to sources outside the control of the institution concerned, which will only complicate the crisis, additional costs and engaging a larger number of staff.

Social media can become a space for creating informal partnerships between government and citizen, a very important factor for authorities to consider is creating

[10] *Social Media and Risk Communications during Times of Crisis*, Special Report of expert round table met in Washington, D.C. in March 2009, available at http://www.boozallen.com/content/dam/boozallen/media/file/Risk_Communications_Times_of_Crisis.pdf, accessed at September 7 2014.

dedicated areas to mobilize volunteers and gather information from citizens that would be useful in crisis management.

In social media there are frequent instances of official communication that interferes with the flow of false information on the crisis from secondary sources or knowingly released. When posting of such information on official websites, the position of the authorities should be a balanced one based on warnings on other sources of misinformation and constant updates and useful information on the developments of the crisis.

Practice has proved that deleting messages, blocking the access to the page or aggressive dialogue from the authorities do not limit the spread of such information in social media since they can be broadcasted shortly on other sites.

Conclusions

With all the dangers associated with it, social media communication has become a mandatory element for institutions, whether in situations of crisis or not, that will shape in the long-term the way in which we structure and use this tool for dissemination of public messages.

As proven above, having a coherent communication strategy through social media provides authorities many advantages, but the most important change is that the citizen becomes a participant in resolving the crisis.

For effective management of the communication in times of crisis, virtual communication through own sources, it is necessary to be built according to the principles of integrated communication within the organisation.

It is important that a government focuses on the effects, on the target audience and influence over it, to determine the most appropriate form of communication at any given time.

Whatever the subject, we need to establish appropriate opinion leaders for each target audience to add credibility to the message and make it efficient.

In any strategy it will be essential to create the necessary capabilities ample reaction from the government, which includes a focus on infrastructure, creativity, flexibility, and management.

Acknowledgement:

This paper is made and published under the aegis of the Research Institute for Quality of Life, Romanian Academy as a part of programme co-funded by the European Union within the Operational Sectorial Programme for Human Resources Development through the project for ***Pluri and interdisciplinary in doctoral and post-doctoral programmes*** Project Code: POSDRU/159/1.5/S/141086

Sectoral Operational Programme Human Resources Development 2007-2013
Project Title: Pluri and interdisciplinarity in doctoral and post-doctoral programmes
Editor:
Publishing date:
The contents of this material do not necessarily represent the official position of the European Union or the Romanian Government.

BIBLIOGRAPHY:

1. BAER, Jay, *Don't Be Scared, Be Prepared – How to Manage a Social Media Crisis*, available at www.convinceandconvert.com/social-media-strategy/dont-be-scared-be-prepared-how-to-manage-a-social-media-crisis, accessed at September 6, 2014, article.
2. BENNETT, Shea, *Twitter, Facebook, Youtube, Google, Instagram, Snapchat – The Internet In Real Time [INFOGRAPHIC],* 26.05.2014, available at www.mediabistro.com/alltwitter/internet-real-time_b57420, article.
3. BURNS, Smith, *The Link between Crisis Management and Social Media*, available at www2.agilityrecovery.com/the-link-between-crisis-management-and-social-management, article.
4. CAVAZZA, Frederic, *Social Media Landscape 2014*, 22.05.2014, available at www.fredcavazza.net/2014/05/22/social-media-landscape-2014, article.
5. COHEN, David, *2Q EARNINGS: Facebook Has 1.32B MAUs, 1.07B Mobile MAUs, 399 M Mobile-Only MAUs*, 26.07.2014, available at allfacebook.com/2q-2014-earnings_b133449, article.
6. COLLINS, Katie, *Government at risk of losing its way with digital strategy*, 04.04.2014, available at www.wired.co.uk/news/archive/2014-04/04/digital-disruption-government, article.
7. COOMBS, Timothy, W., *Comunicarea de criză. O analiză a Institutului American de PR (IPR) Partea a II-a*, available at la http://www.pr-romania.ro/articole/comunicare-de-criza/280-comunicarea-de-criza-partea-a-II-a.html, article.
8. FURGISON, Lisa, *How To Handle a Crisis on Social Media*, available at www.verticalresponse.com/blog/handling-crisis-on-social-media, article.
9. *Government Communication Plan 2014/15*, available at https://gcn.civilservice.gov.uk/wp-content/uploads/2014/05/Government-Communications-Plan_201415_webSmll.pdf, official document.
10. HALSALL, Adele, *The 5 Step Guide To Using Social Media in Crisis Management*, 26.06.2014, available at www.jeffbullas.com/2014/06/26/a-5-step-guide-to-using-social-media-in-crisis-management, article.
11. HANGANU, Alin, *Ambasadorul britanic în România: Pentru mine, social media a fost un experiment de succes*, available at http://digitaldiplomacy.ro/ambasadorul-britanic-romania-pentru-mine-social-media-fost-un-experiment-de-succes, article.
12. LEWIS, Gerald; LAAD, Gitanji, *Role of Social Media in Crisis Communication*, January 2014, available at http://www.geraldlewis.com/publications/ Role_of_Social_ Media_in_Crisis_Communication_Jan_2012_Gitanjali_Laad.pdf, article.
13. WENDLING, Cécile; RADISCH, Jack; JACOBZONE, Stephane, *The Use of Social Media in Risk and Crisis Communication*, in OECD Working Papers on Public Governance no 25, OECD Publishing, 2013 available at http://www.pavillon-orange.org/blog/wp-content/uploads/2013/12/The-Use-of-Social-Media-in-Risk-and-Crisis-Communication.pdf, article.
14. *Social Media and Risk Communications during Times of Crisis,* Special Report , expert round table met in Washington, D.C., March 2009, available at http://www.boozallen.com/content/dam/boozallen/media/file/Risk_Communications_Times_of_Crisis.pdf, accessed September 12, 2014, report.

INDIA'S EFFORTS TO BECOME A GLOBAL POWER: SOME IMPORTANT MILITARY-STRATEGIC ELEMENTS

Florin DIACONU
PhD, Associate Professor, Faculty of Political Science (FSPUB), University of Bucharest
and Senior Researcher (CR II / CS II) with the Romanian Diplomatic Institute (IDR).
E-mail address: florin.diaconu@fspub.unibuc.ro

Abstract**:** *Along the past few years, India managed to get impressive results in the process of consolidating and strengthening the military-strategic components of its national power. With a very large population and a huge economic potential, more and more supported by important global action capabilities of all sorts (including an increasingly potent military arsenal), India might become, in the foreseeable future, one of the really major players on the world arena. We estimate that, along the next few years, the Indian influence and ambitions on the international arena are going to grow fast, strongly boosted by both the need to balance China at all costs, and by the need to be better prepared than ever before for any type of possible negative security and strategic evolutions in the entire AfPak region, which is lacking stability and predictability*.

Keywords: *India; China; Pakistan; national power; strategy; geo-strategic competition; resources.*

At this very moment, the pace of evolution and development of the Indian *global* capabilities of all sorts, *including several geo-strategically significant components of the Armed Forces*, is simply breathtaking. Such an evaluation is not at all to be regarded as an empty figure of speech. On the contrary, it says a lot about one of the emerging *world* powers, which is – most probably – going to play an increasing role on the global arena.

1. The accelerated development of India's military *strategic* assets

In order to better understand the accelerated pace of the quantitative and qualitative growth of Indian military (including *strategic*) capabilities, let us briefly explore a set of very recent news, posted along a very limited time span, of only two days (September 1 and September 2, 2014), on an intensely specialized webpage called *Bharat Rakshak: The Consortium of Indian Military Websites*[1].

On September 1, a piece of news said that the Indian government has decided to purchase "two separate types of US-produced specialised helicopters, one used in attack role and the other for lifting heavy load". The contract will have a total value of "$ 2.5 billion". The same source says that India "accepted the proposals" of *Boeing* "that will supply these copters – 15 heavy lift *CH47F Chinook* and 22 *AH-64-D Apache* — meant for the newly created Mountain Strike Corps", and that "the US copters won the bid in an open competition beating the Russian-built *Mi-26* and the *Mi-28-H*"[2].

[1] The part we are directly quoting and commenting of the webpage we are speaking about can be accessed at the Internet address http://www.bharat-rakshak.com/NEWS/.

[2] "US copters for Mountain Strike Corps", and "Boeing to supply 37 choppers", *The Tribune*, August 29, 2014, posted on September 1, 2014 at the Internet address http://www.bharat-rakshak.com/NEWS/nEwsrf.php?newsid =21238.

On the same day, another open source published a piece of news dealing, among other topics, with the long-term evolution of the Indian Navy. It says that "India's leading shipyard Garden Reach Shipbuilders and Engineers Ltd (GRSE) is now eyeing to tap export market", by means of "exporting an off-shore patrol vessel to Mauritius". A senior military official says that other "four or five more countries are in talk" with the same shipbuilder for other important contracts. The same senior official also declared that "GRSE will be developing 44 warships in next 10 years, including 16 at its Kolkata shipyard". The same open source quoted another high official, who said that "no nation can aspire to be powerful to reckon with on borrowed strength"[3].

Also on September 1, 2014, Ashok Malik, an influential Delhi-based political commentator, published an article dealing with India's oceanic destiny. Malik states that "twice in recent weeks, Prime Minister Narendra Modi spent significant time on new acquisitions of the Indian Navy. He visited the aircraft carrier *INS Vikramaditya* and then commissioned *INS Kolkata*, the largest warship built in India", and that "bolstering maritime security for both military and trade purposes…. is crucial for India; after all, more than 90% of its international trade is dependent on the sea". The author also underlines that "more recently, India has woken up to securing its claims as a paramount naval power in the Indian Ocean before the Chinese surge proved too much". The basic solution India might adopt in order to prevent a too strong enlargement of China's sphere of influence is "the creation of a new city and infrastructure in the Andaman and Nicobar Islands – this could be India's Pudong, India's Singapore, India's Hawaii, whatever you want". The conclusion is that this project could transform India into a "serious power in the Indian Ocean and Southeast Asian region", and that "when it comes to national security, Pakistan represents a tactical challenge; China is the longer-term and strategic challenge", so that "in some senses, the [national] defence lies in the Indo-Pacific, the Indian Ocean…, just off the Andaman and Nicobar Islands. What India does – or doesn't do – on those Islands will determine its destiny in the 21st century"[4].

On September 1, *The New Indian Express* reported that "India is all set to achieve self-reliance in testing of armoured vehicles, as Asia's first Ballistic Research Centre will soon be functioning at Gujarat Forensic Science University (GFSU)" in Gandhinagar. A senior official declared that "we are open to provide services to other countries also, including our neighbours". Testing procedures were briefly presented[5].

On the same day, the same *New Indian Express* published another article also dealing with important military-strategic issues. The article states that the Defence Research and Development Organisation (DRDO) is going "to ensure delivery of cutting edge weapon systems to the Armed Forces in time so that the country can keep pace with other nations in the national security arena". More precisely, "the DRDO plans to test nuclear capable *Agni-I*, sub-sonic cruise missile *Nirbhay* and longest range *Agni-V*". The newspaper reports that *Nirbhay* has a range of 1,000 km, and that "the next generation missile *Agni-VI*" will have "a range of more than 8,000 km"[6].

---

[3] For all these see "GRSE eyeing to tap export market: CMD", in *Business Standard*, August 30, 2014, posted on September 1, 2014, at the Internet address http://www.bharat-rakshak.com/NEWS/newsrf.php?newsid=21240.

[4] Ashok MALIK (Delhi-based political commentator), "Our string of islands theory", in *Hindustan Times*, written on September 1, 2014, and posted on September 1, 2014, at the Internet address http://www.bharat-rakshak.com/NEWS/newsrf.php?newsid=21241.

[5] *PTI*, "Gujarat to Get Asia's First Ballistic Research Centre", *The New Indian Express*, September 1, 2014, and posted on September 1, 2014, at the Internet address http://www.bharat-rakshak.com/NEWS/newsrf.php?newsid=21243.

[6] Hemant Kumar ROUT, "More Tests on DRDO Radar", *The New Indian Express*, updated on September 2, 2014, posted on September 1, 2014 at at the Internet address http://www.bharat-rakshak.com/NEWS/newsrf.php?newsid=21244.

Also on September 1, *IBNlive* published an illustrated presentation of the seven major commando units of the Indian armed forces. The text starts by stating that "the Indian armed forces is a combination of the all the military forces including the Indian Army, Indian Navy, Indian Air Force and Indian Coast Guard. With 1.3 million soldiers, Indian has the world's "third largest military force and the largest standing volunteer army in the world". Then commando units are listed, some of them employed in *strategic* missions – defense of vital infrastructure or fighting terrorist entities"[7].

On the same day, the *Consortium of Indian Military Websites* published a quite long text dealing with the country's efforts aimed at developing its own ballistic defense system. The author says that the system will "provide credible capability against theatre ballistic missiles (TBM) launched from up to 2,000 kms away", and that in the next few years DRDO will develop "two new interceptors… capable of neutralizing RVs delivered by ballistic missiles fired from more than 5,000 km away". The final lines of the text indicate that "this means that India has all the elements in place for a direct ascent counter space system that can easily be used for anti-satellite purposes"[8].

And one day later, on September 2, *Business Standard* published an article dealing with the newest combat ship to be commissioned by the Indian Navy. It is the "Offshore Patrol Vessel *INS Sumitra*", and a Defence Ministry release said that "the induction of *INS Sumitra* in the Eastern Naval Command and her basing at Chennai will enhance the offshore surveillance and maritime patrolling capability on India's eastern seaboard in addition to giving a fillip to anti-piracy operations actively being undertaken by the Indian Navy". The ship has "a displacement of about 2,200 tonnes" and an "impressive weapon and sensor outfit"[9].

If are to summarize all these pieces of news along the two days we have been speaking about (September 1 and 2, 2014), the basic elements are these ones: eight pieces of news, *all* of them significant at several levels, including the *strategic* one (and most of them at *geo-strategic* level as well). Three texts are directly dealing with the Navy (including one speaking about *geo-strategic competition with China*); two of them are dealing with ballistic weapons (offensive ones, with a range up to 8,000 kilometers, or modern defensive ABM systems); one of them is speaking about both a strong partnership with the U.S., and increased helicopter capabilities (including attack aircraft, and heavy transport ones – these are a major *strategic* asset, at least in the mountains and high hills on the Chinese and Pakistani borders); one of them is dealing with advanced military testing facilities; and another text is dealing with commando (Special Forces) units, which can be deployed in various contexts, including some which clearly are *geo-strategically significant*). *Put together, these texts generate a vivid image (even if it is a partial one, it can be easily extrapolated to better understand long-term trends, using what literature studies and analysis call 'pars pro toto' method) of the impressive might, goals (including the geo-strategic ones) and evolution of the Indian armed forces*.

[7] For all these see "The smart Black Cat commandos and the safari suits of SPG commandos: 7 Indian armed forces uniform codes that you need to know", *IBNLive*, September 1, 2014, posted on September 1, 2014 at the Internet address http://www.bharat-rakshak.com/NEWS/newsrf.php?newsid=21245.

[8] Saurav JHA, "Some notes on DRDO's PDV ballistic missile defence interceptor", *IBNLive* (and *Geek at Large*), August 30, 2014, posted on September 1, 2014, at the Internet address http://www.bharat-rakshak.com/NEWS/newsrf.php?newsid=21246.

[9] Press Trust of India, "Navy to commission INS Sumitra on September 4", *Business Standard*, September 2, 2014, posted on September 2, 2014 at the Internet address http://www.bharat-rakshak.com/NEWS/newsrf.php?newsid=21247.

2. Some remarks on India's national power: strengths and vulnerabilities

National power of India has *sharply increased* along the past decades. At the beginning of the century, for example, its total *demographic resources* already reached more than 1 billion inhabitants (five times larger than 100 years before, in 1901), and its GDP / capita was 1,800 U.S. dollars[10]. In 2001, reports a recent and serious French collective study, GDP / capita already was increasing, as a result of quite many years of positive economic growth[11]. Along a few decades, foreign private direct investments have been 'skyrocketing', from 1.2 billion U.S. dollars (in 1980-1990) to 40-50 billion (in 1991-2005)[12], which means a 4,000 % growth rate along less than a generation.

Another strategically significant positive asset of India is the *very large number of university students*: all Indian universities, together, had 9.2 *million* students in 2004[13] (a figure larger than 50 % of the total population of Romania, or matching total demographic resources of Hungary or Bulgaria). Even if only 10 % of them are really good quality students, this means that, each year, Indian economy (including the defence sector, and the armed forces, and various strategic R&D facilities) have direct access to at least 30 or 40 thousand good and very good (and some of them exceptional) young specialists. Such human resources can – even if they might be severely diminished by quite intense 'brain drain' absorbing many skilled specialists of all sorts in either Indian private sector, or even in other countries –support a decent growth pace of both the Indian armed forces and of the Indian industrial and R&D defence sector.

Speaking about *vulnerabilities and weaknesses of India's national power*, a long-term one has been, for several decades, the diminishing share of India's contribution to the global economy. In 1950, India generated roughly 12 % of the industrial production of the group of developing countries (the so-called 'third world'). 30 years later, in 1980, the share of India's industrial production in the same group of national economies reached only 4.5 %[14]. Another major vulnerability is the fact that, mainly after 1980, *the oil and gas deficit grew larger and larger*, as a result of the sharp increase of national demand (boosted by impressive growth), while domestic supply was limited: in the last two decades of the 20th century, India consumed in each year 120 million tons of oil, and produced only 33 million tons[15].

More recently, in 2001-2002, the country was also confronted, according to a large study written by three Romanian authors, with other significant vulnerabilities: a *very large foreign debt* (almost 100 billion USD in late 1990s, and *high inflation ratio* – 10 %, in most of the years after 1990.[16] *Poverty and regional underdevelopment* still remain a major problem, with both immediate and long-term consequences: after decades of intensive efforts: less than 15 years ago, in 2001, 192 million families could afford only one room, and 17 % of the population had no source of safe drinking water in proximity. A large problem is also *the 'development gap' separating urban and rural areas*: 25 % of the urban families have at least a bicycle or a scooter, while only 7 % of the rural families can afford this. 23 % of the houses

[10] Horia C. MATEI, Silviu NEGUT, Ion NICOLAE, "India", in *Statele lumii de la A la Z*, Editura Meronia, Bucureşti, 2002, pp. 256-261.
[11] Christophe JAFFRELOT (main editor), *L'inde contemporaine, de 1950 a nos jours*, Fayard et CERI, Paris, 2006, p. 164.
[12] Christophe JAFFRELOT (main editor), *op. cit.*, p. 166.
[13] Christophe JAFFRELOT (main editor), *op. cit.*, p. 162.
[14] Christophe JAFFRELOT (main editor), *op. cit.*, p. 130.
[15] Christophe JAFFRELOT (main editor), *op. cit.*, p. 149.
[16] For these figures in 2001-2002 see Horia C. MATEI, Silviu NEGUT, Ion NICOLAE, "India", in *Statele lumii de la A la Z*, Editura Meronia, Bucureşti, 2002, pp. 256-261.

in towns have access to traditional telephonic services, while only 4 % of those in the villages have access to them[17].

Some other strengths and weaknesses deeply influencing national power of India could have been listed here, but I've already done this, with many details, a few years ago, in a study published by a Romanian journal specialized in global affairs[18].

3. Role of armed forces as major element of India's national power: developing long-range and global capabilities

The armed forces are, anytime and anywhere, a major element of the national power, say major Realist authors[19] And we strongly underline that the evolution of India's armed forces along the past few decades is also *really* impressive (we are speaking about a long-term and continuous process which was – and is – supported by a huge demographic potential, by reasonably long periods of economic positive growth, and by a *strong and remarkably coherent political will*). In the opening stages of the existence of independent India, the country had some 280,000 military personnel, with limited strategic capabilities. *60 years later, the same country already had 1.1 million soldiers in the Army alone*, plus 170,000 men in the Air Force (*the fourth largest in the world*), plus 55,000 in the Navy (which is, with its more than 100 ships, *the sixth largest in the world*)[20]. India also has a *significant nuclear and ballistic arsenal*[21].

Some elements allowing a better understanding of India's military power have already been presented along the first pages of this study. Now we are going to explore another topic: the way in which India, already a major regional power, is developing new military 'tools', with long range, and able to project national power *very* far away from the borders. *Quite clearly, developing long-range or globally capable military means of all sorts is one of the very clear 'signs', showing any attentive observer that a certain actor on the international arena is deliberately preparing for a major status change (or 'upgrade') – trying not to be just a regional power any more, but to become a global one* (what Martin Wight called some years ago a 'world power'[22])

From a quite long list of such devastatingly powerful (and geo-strategically significant) *long-range* military means India already has (and is trying to develop even more) we are going to briefly evaluate here, with only a few illustrative details, three categories: *strategic air forces, aircraft carriers and nuclear submarines*.

At this very moment, India has some *Tu-142* (a variant of the *Tupolev Tu-95 'Bear'*) "strategic, intercontinental heavy-payload bomber aircraft". This *quite obsolete* aircraft "has a maximum level speed of 650 km per hour and an unrefueled combat radius of 6,400km. With one in-flight refuelling, the aircraft has a combat radius of 8,200km". According to open sources, "the Indian Air Force 312 Squadron based at Arkonam operates eight *Tu-142MK-E*

---

[17] For the figures offering a vivid image of poverty and underdevelopment, see Christophe JAFFRELOT (main editor), *op. cit.*, pp. 160-161.

[18] Florin DIACONU, "India, superputerea de mâine, încă în leagăn", in Revista *de politică internaţională*, an I, nr. IV, Bucureşti, 2006, pp. 29-40.

[19] Hans J. MORGENTHAU, *Politics among nations: The struggle for power and peace*, third edition, Alfred A. Knopf, New York, 1964, pp. 118-121.

[20] "Chapitre XI: Les forces armees indiennes", in Christophe JAFFRELOT (main editor), *op. cit.*, p. 248; same work offers extensive presentation of the way in which Indian forces are organized – pp. 252-253.

[21] Ian KEARNS, "Beyond the United Kingdom: Trends in the Other Nuclear Armed States Discussion Paper 1 of the BASIC Trident Commission, An independent, cross-party commission to examine UK nuclear weapons policy", *British American Security Information Council* (*BASIC*), November 2011, .pdf text at the Internet address http://www.basicint.org/sites/default/files/commission-briefing1.pdf, pp. 25-26.

[22] Martin WIGHT, *Politica de Putere*, Ed. Arc, Chişinău, 1998, pp. 62-68.

Aircraft". These eight bombers "entered service in the Indian Air Force in 1986" and are "equipped for maritime patrol and anti-surface warfare, reconnaissance and search and rescue". Their maximum speed exceeds that of earlier variants, reaching "920km per hour", and the maximum "range is 15,000km"[23].

The *Indian Air Force is trying to become a major and fully developed long-range strategic force*. A quite recent text states all "nations following the employment of airpower predominantly in tactical role – Germany, Japan, Italy, erstwhile USSR lost in World War II", while "USA, UK using airpower in strategic role won the war outright". The same text also states that "now the advances in technology have made modern air power extremely accurate and far reaching - with global reach for the mighty". The same author speaks about the "strategic nature in airlift" operations, and states that "as one looks at advances in air power capability and its virtue of stealth, precision, increasing speed and range, and contribution of space, one can understand the increasing 'strategic' nature of Air Power, thus of the IAF". This very 'strategic' nature means several major features, including "precision attacks over vast distance" and "rapid mobility over large distance". The general conclusion is that strategic air forces are a must for any actor with global interests, and "any nation that ignores this aspect stands to be devoid of this instrument of 'Strategic Choice'"[24].

India clearly plans to buy – or to manufacture – some other *long-range* bombers. A few years ago, "Russia has offered to sell several long-range *Tupolev Tu-22M3* bombers to India" – these planes have a range of 7,000 kilometres[25]. The political and media debate over strategic bombers is intense too. A quite recent text states that "while China is bolstering its already strong strategic bomber fleet (of *Xian H-6K* aircraft) by buying off the production line of the most advanced *Backfire*, the *Tu-22 M3*, and prioritising the indigenous development of the four-engined, wing-shaped, *H-18* strategic stealth bomber, IAF hopes its *Su-30*s assisted by aerial tankers will be a credible deterrent and counter against the Chinese bomber armada". The same author also states that "it will be prudent for the IAF, even at this late stage, to constitute a Bomber Command and cadre, lease ten or so *Tu-160 Blackjacks* from Moscow and… invest in a programme jointly to design and produce with Russia the successor aircraft to the *Blackjack* — the *PAK DA*, which is expected to fly by 2025. I have long advocated acquisition of a bomber because, compared to strike fighters and ballistic and cruise missiles it has far more strategic utility, including in nuclear signalling, crisis stability, and escalation control"[26]. A quite recent interview with Air Chief Marshal NAK Browne offers an even clearer image of long-term plans of the Indian military. The senior military official says that "IAF has embarked on a modernisation programme aimed at transforming itself into a potent strategic force". Browne also says that "we would have gradually built-up our capability to face future challenges of a two and half front war", and that "the IAF aims to equip itself with a good airlift capability, extended reach and special operations capability by induction of

[23] "Tu-95 Bear Strategic Intercontinental Bomber, Russia", on the webpage called *airforce-technology.com*, at the Internet address http://www.airforce-technology.com/projects/tu95bear/, accessed on September 1, 2014

[24] Air Vice Marshal AK TIWARY, "IAF: The Strategic Force of Choice", in *Indian Defense Review*, Issue Vol 22.3 Jul-Sep 2007, at the Internet address http://www.indiandefencereview.com/news/iaf-the-strategic-force-of-choice/0/.

[25] "Russia offers TU-22M3 strategic bombers to India", *DefenceTalk: Global Defense, Aerospace & Military Portal*, December 8, 2005, at the Internet address http://www.defencetalk.com/russia-offers-tu-22m3-strategic-bombers-to-india-4373/ .

[26] Bharat KARNAD (Professor at Centre for Policy Research), "Strategic Bomber for IAF", *The New Indian Express*, February 7, 2014, text accessed at the Internet address http://www.newindianexpress.com/columns/Strategic-Bomber-for-IAF/2014/02/07/article2042008.ece.

Very Heavy Transport Aircraft, Flight Refuelling Aircraft and Special Ops Aircraft respectively"[27]

Significant efforts were also made in order to develop long-range airlift capabilities. A few months ago, an already quoted text underlined "the statement of the new Chief of the Air Staff, Air Chief Marshal Arup Saha, who talked of his service achieving a "strategic" profile in terms of its ability to pull 'expeditionary' missions", using a "growing numbers in the inventory of *C-17* and *C-130J* transport planes"[28].

Another geo-strategically significant feature of the Indian armed forces is the serious effort made in order to get, operate, and develop a strong aircraft carrier force, with almost global capabilities. Recently, "in its first major military decision since taking office, the new Indian government is backing the completion of India's first indigenously-built aircraft carrier". The governmental decision allocated "approx. $3.1 billion to complete the construction of the *INS Vikrant*". The open source we are quoting here also says that this ambitious program is, together with other ones, "plagued by lengthy delays usually caused in part by excessive amounts of bureaucracy". Anyhow, according to the new schedule, the carrier will start "extensive sea trials sometime in 2016" and will be "inducted into the navy by the end of 2018". Powered gas turbines, "the ship will be about 40,000 tons with a length of 260 meters and breadth of 60 meters" and it "will carry among other things the *MiG-29K*, Light Combat Aircraft *Tejas* and *Kamov 31* helicopters". At this very moment, Indian Navy operates "the *INS Vikramaditya*, the refitted Russian carrier that was delivered to India last year. India paid $2.33 billion for the 44,000 ton former *Admiral Gorshkov*, which Russia's Navy used from 1987 through 2005", and is still using "the aging British-built *INS Viraat* (*R22*) carrier, which India commissioned in 1987 (England commissioned it as the *HMS Hermes* (*R12*) in 1959 and decommissioned it in 1984). It is expected to be decommissioned in the coming years. India also has a 60,000-tonne IAC-II project that is currently in the planning stages"[29]. *When both INS Vikrant and the future IAC-II carrier will be operational, India will have at least two, or maybe three fully functional carriers – while the US has at this very moment 10, and China has only one*.

Some critics speak about "the aircraft carrier's high vulnerability (to new disruptive weapons and technologies)", and say that "inadequate logistical sustainability render it an irrelevant asset". But "finally, and most significantly, a navy needs assets for 'power projection' – a critical component of a nation's maritime strategy. Power projection assets are an embodiment of a nation's strategic capability and political intent. Navies strive to accrete power and project it far beyond the home country as a metric of national influence and their own regional relevance. Aircraft carriers fall into this category", a recent Indian text says. It also states that carriers "the arrival of an aircraft carrier at a regional port of call imparts a diplomatic impact that cannot be matched by a submarine or a destroyer. Therefore, even while acknowledging the flexible demands of future maritime missions on maritime forces that would necessitate a shift towards multi-purpose warships (such as amphibious assault vessels), the likelihood that aircraft carriers would continue to be relevant in their present form and configuration, remains high". The same text says that "the Indian Navy will also be mindful of the maritime ambitions of the People's Liberation Army Navy (PLA-N) and the role that its new aircraft carrier – the *Liaoning* – is likely to play in China's Indian Ocean expansion". *The conclusion of the text (written by a research scholar at the Institute for*

[27] "Exclusive Interview of Chief of Air Staff", on the *DSA (Defence and Security Alert)* webpage, at the Internet address http://www.dsalert.org/aerospace-power-in-india/289-exclusive-interview-of-chief-of-air-staff, accessed on September 4, 2014.
[28] Bharat KARNAD (Professor at Centre for Policy Research), *op. cit.*
[29] Zachary KECK, "India's Modi Approves Aircraft Carrier Funding", *The Diplomat*, July 11, 2014, at the Internet address http://thediplomat.com/2014/07/indias-modi-approves-aircraft-carrier-funding/.

Defence Studies and Analyses, whose main area of interest is Maritime Security in the Indian Ocean) is that "if used intelligently", Indian aircraft carriers "could prove to be critical in shaping the Indian Ocean's strategic environment"[30].

Some texts are comparing Indian and Chinese Carrier Battle Groups, saying that the Chinese battle group "'built' around *Liaoning* aircraft carrier" is "characterized by many weaknesses" and underlining that "noteworthy, Indian aircraft carriers will be supported and defended from enemy submarines by eight *P-8I Poseidon* long-range maritime reconnaissance and anti-submarine warfare aircraft."[31]. And other open sources indicate that a significant "Asian aircraft carrier race started", and that a new Japanese aircraft carrier *Izumo* (19,500 tons), plus the larger Indian one(s) might seriously "diminish the Chinese challenge" in the Pacific and Indian Ocean. The same text also states that India's carriers might be enormously useful in case of war – "for instance against Pakistan"[32].

The third element to be seriously taken into account in our debate is the increasing number of India nuclear submarines. With a practically unlimited range, and armed with nuclear weapons, these submarines are potent tools with obvious geo-strategic meaning, allowing the Indian interests to be present in any part of the World Ocean. In November 2011, Ian Kearns wrote that "on 26 July 2009, India also launched its first SSBN, the *Arihant*" and that "four other submarines are reportedly planned"[33].

More recently, in March 2014, media reports indicated that "the [Indian] navy operates a solitary *Akula* class SSN, *INS Chakra*, leased from Russia in 2012", that "only seven of India's fleet of 13 conventionally powered submarines are operational", and that "the *Arihant*, the first of three indigenously built nuclear powered ballistic missile submarines (SSBNs) is yet to commence sea trials". The same source said that Indian strategic planners are strongly disturbed by China's decision to deploy, for several months, a nuclear submarine to the Indian Ocean and are afraid that along the next few years Beijing is going to send near India an entire carrier battle group[34].

Brief conclusions

Demographic and territorial dimensions place India on a top position among the great powers. With a sharply increasing economy, *India has the necessary resources to develop an impressive military arsenal, including several geo-strategically significant assets –long-range Air Force units, several aircraft carriers, plus nuclear submarines, ballistic missiles and nuclear weapons. These military assets can, up to a certain point, play a role not only within the regional arena, but on the global one as well.*

We estimate that, along the next few years (10 to 20), India's role on the global arena is going to sharply increase. At least three factors make such a forecast a very probable one: increasing need of vital resources from abroad; the clearly increasing geo-strategic competition with China, a country also badly needing vital resources from abroad and competing for the control of the same vital sea routes India has to rely on; and thirdly, the

[30] Abhijit SINGH, "INS Vikramaditya and the Aircraft Carrier Debate", *The Diplomat*, December 10, 2013, at the Internet address http://thediplomat.com/2013/12/ins-vikramaditya-and-the-aircraft-carrier-debate/.
[31] David CENCIOTTI, "Photo of India's new Aircraft Carrier Battle Group. Better than China's?", January 06, 2014, at the Internet address http://theaviationist.com/2014/01/06/indian-navy-aircraft-carriers/.
[32] Donald KIRK, "Asian Aircraft Carrier Race – China Vs. India Vs. Japan", in *Forbes*, August 13, 2013, at the Internet address http://www.forbes.com/sites/donaldkirk/2013/08/13/aircraft-carriers-first-chinathen-india-and-japan-all-want-one/.
[33] Ian Kearns, *op. cit.*, p. 26.
[34] For all these see Sandeep UNNITHAN, "Exclusive: Indian Navy headless as Chinese nuclear sub prowls Indian Ocean", *India Today*, March 21, 2014, at the Internet address http://indiatoday.intoday.in/story/indian-navy-chinese-nuclear-sub-indian-ocean/1/350498.html.

very probable long-term lack of regional security, stability and predictability in the entire AfPak (Afghanistan and Pakistan), a feature of the surrounding strategic landscape which naturally worries India a lot. We think that, *the more potent these three challenges are going to become, the stronger will be the need for India to become a fully active world power*. In such a situation, *its globally capable military assets might become more important than today, and most probably they will get extra resources allowing a quick and massive development* (world history shows that a sharp increase of the military might accompanies, in most occasions, power status 'upgrades', for example those leading from great power status to world power status).

BIBLIOGRAPHY:

1. JAFFRELOT, Christophe (main editor), *L'inde contemporaine, de 1950 a nos jours*, Fayard et CERI, Paris, 2006.
2. KARNAD, Bharat (Professor at Centre for Policy Research), "Strategic Bomber for IAF", *The New Indian Express*, February 7, 2014, text accessed at the Internet address http://www.newindianexpress.com/columns/Strategic-Bomber-for-IAF/2014/02/07/article2042008.ece .
3. KEARNS, Ian, "Beyond the United Kingdom: Trends in the Other Nuclear Armed States Discussion Paper 1 of the BASIC Trident Commission, An independent, cross-party commission to examine UK nuclear weapons policy", *British American Security Information Council* (*BASIC*), November 2011, .pdf text at the Internet address http://www.basicint.org/sites/default/files/commission-briefing1.pdf.
4. MALIK, Ashok (Delhi-based political commentator), "Our string of islands theory", in *Hindustan Times*, written on September 1, 2014, and posted on September 1, 2014, at the Internet address http://www.bharat-rakshak.com/NEWS/newsrf.php?newsid=21241.
5. MATEI, Horia C., Silviu NEGUT, Ion NICOLAE, "India", în *Statele lumii de la A la Z*, Editura Meronia, Bucureşti, 2002.
6. MORGENTHAU, Hans J., *Politics among nations: The struggle for power and peace*, third edition, Alfred A. Knopf, New York, 1964.
7. TIWARY, AK, Air Vice Marshal, "IAF: The Strategic Force of Choice", in *Indian Defense Review*, Issue/Vol. 22.3, July-September 2007, text accessed at the Internet address http://www.indiandefencereview.com/news/iaf-the-strategic-force-of-choice/0/.
8. WIGHT, Martin, *Politica de Putere*, Ed. Arc, Chişinău, 1998.
9. A significant number of media reports, each of them with author's name, complete title and Internet address, in footnotes. Not present here simply because the limited available space.

DEMOCRACY IN THE MIDDLE EAST: TOWARDS A MORE PECULIAR FRAMEWORK OF ANALYSIS

Ecaterina MATOI
PhD candidate and research assistant within Defence and Security Faculty, "Carol I" National Defence University, Bucharest, Romania; PhD student in Islamic and Middle Eastern Studies (MUBIT) at the University of Basel, Switzerland.
E-mail address: matoi.ecaterina@myunap.net

Abstract: *For several decades, an already classical controversy has been developed, regarding the compatibility between democracy, in its forms developed by Western political culture (real partitioning of power within the state and independence of institutions, constitutionalism, respect of human rights and liberties, liberty of expression, existence of an active civil society, normal relations between state and society etc.) and capacity of the state and society from the Arab-Muslim World to functionally assume such a model. In the case of latter, a series of characteristics is linked to authoritarian and patriarchal political transitions, to persistence of an economic, political and religious violence which affects the internal stability of society, the important role of army which interferes or even dominates the civilian political environment, fluidity of the national realities and attachments which are challenged by the persistence of certain ethnic, sectarian or regional solidarities, raising issues on the legitimacy of nation-states, projects of Islamist movements that promote their own models of state and society, constructed from a reinterpretation of Islamic tradition, etc. Based on these assumptions, in this paper I intend to review several specific elements that contribute to the regional conditioning of democratization processes, especially in the context of new political and security dynamics, after the Arab Spring, the possibilities of democratization in the Middle East and North Africa, which have experienced tendencies of authoritarianism and especially an ascending fragmentation of the state order and stability, that has emerged as one of the recurrent analysis themes for specialists and decision makers.*

Keywords: *Middle East and North Africa, democratic systems, authoritarian political culture, Islam.*

1. State, *asabiyya* and the (im)possibilities of democratic systems in Arab-Muslim World

Democratizing the Middle East is linked to history of its formation in modern times, but also to its real capacity to assimilate the values of Western modernity, to which the themes of democracy, turned universal, belong with all implications. They are: the existence of a political and social space designed to defend and reflect individual and collective interests, free elections, a genuine separation of the powers of the state, functional institutions having an objective manner of governing, the existence of a civil society and of civil awareness, etc. This entire democratic political culture, which developed within the political philosophy and historical dynamics pertaining to the European space, gradually became, particularly after the eighteen century, a normative and universal model. The model was exported or assumed on an increasingly larger scale in different geographical areas where it encountered and had to be adjusted to different traditions and different cultural and political experiences. One could have expected that, in Middle East and North African region, the

political and cultural proximity of the West are a catalyzing factor able to facilitate the emergence of a native democratic space in the area, at the beginning of modern times. Actually, and this is the cause that has conditioned until today region's democratic deficit, the contacts between systems of values belonging to the modern West and those pertaining to different parts of this area have often been marked by mistrust, rivalries, conflicts, successive assimilation and rejection, and above all adjustments, in accordance with circumstances and interests.

Therefore, the difficulty of creating a democratic culture in the Muslim-Arab World has both endogenous and exogenous causes. Depending on different schools of analysis, some defend an essentialist perspective, maintaining the principle according to which political culture and specific Muslim religious traditions could be the determining factors that prevent an integral adoption of philosophical foundations and praxis which established standard democracy[1]. Others, on the contrary, tend to pay attention to different and particular situations of every country and to point towards the plurality of factors, both internal and external, that have generated autocratic situations and made the development of real and functional democratic spaces difficult[2]. Such epistemological controversies, which impact upon the decision-making activities of political leaders regarding strategies and attitudes toward the area, are, at the end of the day, almost insurmountable because the Middle East has a hermeneutical potential so divergent that makes univocal perspectives impossible. Thus, over the decades, many interpretations and controversies concerning the events and realities in the area followed, both within ranks of an epistemic community of specialists and political factors.

Consequently, every analysis of the democratic condition, of its real possibility and concrete forms it can take, particularly of its objective limits, must have as background the awareness and the fact that values and practices of democracy have been projected in relation to and permanently enter in a modeling interdependence with numerous historical, cultural, religious, anthropological, and political experiences, pertaining not only to the states as such, but also to communities within this area. Actually, the great problem of the Middle East is precisely different trajectories the destinies of different states and societies have received, coming in a plurality of variables mostly in an antinomical and conflictual shape. Modern states in the area are often not the product of any awareness of identity or historical determinism generated by the populations themselves. They are rather artificial constructs of Western powers (Lebanon, Iraq, Syria, Israel/Palestine, Jordan, Libya, and Algeria), or the result of certain political elites emergence, having a tribal or communitarian background, which first take the power and afterwards produce the state´s institutional and decisional structure around their own interests and need to preserve their domination (Saudi Arabia and emirates of the Gulf)[3]. Thus, democratic deficit belongs structurally to the Middle East since incipient moments of its formation as a new system based on the nation-state model, imported from the West.

In the Arab-Muslim area, state – as an official actor that exercises authority, according to the classical theory of political sciences – is growing not only based on a rational project and corresponding to a functional rule that sets relations between citizens and exercise the institutional and objective authority, but is rather the result of rivalries between different

---

[1]Bernard LEWIS, *What Went Wrong? The Clash Between Islam and Modernity in the Middle East*, Harper Perennial, 2003.

[2] Larry DIAMOND, Marc PLATTNER (eds.), *Democratization and Authoritarianism in the Arab World*, Johns Hopkins University Press, 2014.

[3] Christie KENNETH, Mohammad MASAD (eds.), *State Formation and Identity in the Middle East and North Africa*, Palgrave Macmillan, 2013.

particular groups of solidarity, that have ideological and political legitimacy in the state, generated by the advantage of power. Furthermore, Middle Eastern Studies scholars define the state as one of the multiple actors at social and even political level that manages societies from different Arab or Muslim countries. According to Roger Owen, "its reality is much more complex, more fluid and much more difficult to conceptualize"[4] than the state defined by a European model, which is understood as organized and organic entity that exerts the monopoly of power on a certain territory. Monarchs, officers, commercial and religious elites, tribal leaders, political parties are becoming auto-referential structures in competition for seizing authority in the state, but often in a totalitarian logic, taking into account that any political ascension of a group tends to have a permanent character, excluding or suppressing the others and following own interest. This generates the intrastate violence (often transferred into an inter-state violence) in the majority of states from the region and a political rivalry between particular groups of solidarity that augment the motivation of partisanship and mutual apprehension (confessional, ethnic, tribal and geographical identities). Shaping of national states and elaboration of national ideologies that legitimized elites in power have represented a conceptual, social and geopolitical new construction for communities of the Middle East, pertaining from centuries to supranational political systems which favor social construction based on identities generated by religion, ethnos or tribal affiliation. The instauration of nation states and frontiers (thus the limitation and restriction of migratory people´s mobility), and modernization processes affected the traditional social order that defined communities, generating different behavioral and social mutations. These reconstructions of identity based on modern criteria did not totally eliminate the traditional ethnic, religious, and tribal solidarities, but combined them with new forms of communitarization and collective mobilization, such as parties, secret societies and military groups.

According to some scholars, also partisans of the khaldunian theories (Olivier Carré, Michel Seurat), political sciences in the Arab-Muslim must assimilate conceptually and capitalize theoretically the behavioral structures proper to this populations, taking into account they interfere with and structure the classical norms of the institutional and political functionality[5]. The democratization theories, in their Western patterns of analysis, have developed less resources in order to build an explanatory and theoretical framework, enough coherent and functional, and has not identified the modalities that can surmount collective memories and particular attachments of different social groups, so that they can accept the real democratic game and principle of equality between people, no matter their linguistic, tribal, ethics and sectarian identities. The delay in developing a real democracy for the Middle East and North Africa comes as a result of the difficulty in setting both a coherent nation state and national collective identities that assume fidelity for the state and not for different proximate communitarian groups.

2. Military and persistence of authoritarian political culture in the Middle East

It gets to another characteristic of the Arab-Muslim World´s political systems: the importance of military factor, involvement of the military elites in decisional field, either

---

[4] Roger OWEN, „State and Society in the Middle East", *Plenary address to the Twenty-third Annual Meeting of the Middle East Studies Association of North America*, Toronto, 15-18 November 1989, apud Philip S. Khoury, Joseph Kostiner, *Tribes and State Formation in the Middle East*, University of California Press, 1990, p. 6.

[5] Syed Farid ALATAS, „Ibn Khaldun and Contemporary Sociology", *International Sociology*, Vol. 21, No. 6, 2006, pp. 782-795.

directly or indirectly. In this matter, the Middle East is similar to South America, where many of the states have faced similar moments of military coups, followed by the installation of authoritarian and non-liberal regimes, military led. The difference is however important. In Latin America, the emergence of military regimes, between the sixth and eighth decades of last century, was the result of both internal factors (rise of leftist militancy, weakening of civil political elites, need for social security) and especially external (support of the United States to limit region´s evolution towards communism). Furthermore, they represent only a stage in the political history of this region and not a norm; gradually, they will leave room, often voluntarily, for the reinstallation of civil regimes and return to democracy, even if crossed by new specific moments, such as leftist and populist temptations[6].

Instead, however, in the Middle East, with a few exceptions (Tunisia, Lebanon, post-Saddam Iraq), the army was and remained a key actor at political and economic level. Political and social emergence of the army since 19th century was consequence to the lack of a coherent civil society; army was considered more often as a key vector for modernization of societies, substituting some civil political classes considered inefficient or insufficiently attached to national values[7]. In the last age of the Ottoman Empire, army will be the one to push towards westernization of the system and will take over the power, with the Young Turks. In the Kemalist and post-Kemalist Turkey, army itself becomes an instrument for state and society modernization, reformation and, at the same time, trying to control political power, intervening in times when it seems that the republican and laic values are insufficiently assumed[8]. Turkey had been and remained a prototype of this complex dialectic between the tendency to implement a model of democratization as functional as possible (parties, free elections, parliamentarism, separation of state institutions) and the persistence of control mechanisms, institutionalized through the National Security Council, which intervened in political field in order to defend national security, affecting the country's democratic acquis. Iran, during Reza Khan period, went through the same process of authoritarian modernization, where army assumed the role of social reform instrument and ultimate power that ensures persistence of an official civil regime[9]. In the Arab World, especially in post-colonial countries, army becomes an inextricably actor, inspired, most often, by the Kemalist model. The army builds its legitimacy on behalf of the role as resort in defense of national, anti-colonialist values, and assumes defending, directly or indirectly, modernization and governance of their countries[10]. The Nasserian Egypt serves as model but the situation characterizes also history of Iraq until 1968, the post-colonial Algeria, Libya during Qadhafi period, Syria. Military involvement in politics is more obvious in republican regimes, crossed by numerous coups where the army was an essential actor. In the monarchist, conservative systems (Jordan, Gulf monarchies), army is part of the regimes´s defense and broad privileges granted to this institution are, in part, for its loyalty. All these facts, however, are not new in the history of Arab-Muslim regimes; for hundreds of years, the

---

[6]David PION-BERLIN (ed.), *Civil-Military Relations in Latin America: New Analytical Perspectives*, The University of North Carolina Press, 2000.

[7]Khuri FUAD, *The Study of Civil Military Relations in Modernizing Societies in the Middle East: A Critical Assessment*, UCLA Center for International and Strategic Affairs, 1982

[8]Steven COOK, *Ruling But Not Governing: The Military and Political Development in Egypt, Algeria, and Turkey*, Council on Foreign Relations, 2007, pp. 93-132.

[9]Stephanie CRONIN, „The Army, Civil Society and the State in Iran: 1921-26", Touraj Atabaki, Erik Zurcher (eds.), *Men of Order: Authoritarian Modernization Under Ataturk and Reza Shah*, I.B.Tauris, 2004, pp. 130-163.

[10]Elisabeth PICARD, „Arab military in politics: From the revolutionary plot to the authoritarian state", in Giacomo Luciani (ed.), *The Arab State*, University of California Press, 1990, pp. 189-219.

spirit of caste among military structures was an important factor that helped their emergence in political and decisional field, from the Abbasid period, when various emirs are recognized as governors or even founders of dynasties. Developing a true institution of Mamluks, tradition induced, until today, the persistence of a group conscience among the military, which is reflected in its modernized and adapted variants, in current realities of various countries in the region such as Algeria, Syria, Egypt[11].

Thus, it can be concluded that if the military institution was often a factor of modernization and progress on one hand, helping in structuring trans-community national solidarities, on the other hand it has blocked the development of genuine democratic systems, because it serves as a source or instrument for authoritarian regimes, especially in the post-war period[12]. Present Egypt visibly illustrates this reality, for SCAF (Supreme Council of the Armed Forces) has managed to retain the privileges and position in the post-Mubarak period and to influence the social processes and coup that led to the fall of Muhammad Morsi´s regime along with the Muslim Brotherhood. There are currently countless controversies within scientific and political fields, at international level, regarding current situation and fate of Egypt. The existence of a civil political system and an ongoing democratic process at this moment, cannot occult, however, that the army remains an authority determined to control decisional field and to intervene whenever considers that its interests or its internal or foreign customers' interests are threatened by the situations in Egypt[13]. The situation is similar in Algeria, where military and security structures persist after independence, defending the political life and intervening sometimes, when they consider that survival and interests of the political and military official establishment are challenged or threatened, as in the 9th decade, with the electoral success of Islamist movement.

On the other hand, one may say that beyond these anti-democratic excesses, the army's role was crucial for the internal stability and management of numerous external political and military crises, in a climate marked by violence and structural instability such as the one in Middle East[14]. Weakening of military authority may have itself negative consequences on creating a political and security climate to ensure implementation of a democratic system. This was the case of the post-Saddam Iraq, where the total dissolution of army, in 2003, was a key factor of institutional and security disaggregation, blocking country´s recovery and the assumption of a functional democratic acquis for several years. It is the case of present Libya, where the disappearance and difficulty of rebuilding a national army favors not only the persistence of militia and post-revolutionary paramilitary groups that maintain an ongoing climate of violence, but especially the gradual disintegration of national cohesion and political and administrative autonomy of different new local, urban or tribal power structures.

Therefore, when considering army´s role in the transition processes towards democracy or in systems within the Arab-Muslim World, one must always contextualize situations and avoid specific political science generalizations. The army is a key actor for any democratic regime, and in the Middle East, there were moments when military institutions had a very positive role, especially in providing a collective framework to build new national

---

[11]Rut DIAMINT, Barah Mikail, *Militaries, civilians and democracy in the Arab World*, Fride – Policy Brief, January 2012.

[12] F.I. KHURI, „The study of civil–military relations in modernizing societies in the Middle East: a critical assessment", in R. Kolkowicz, A. Korbonski (eds.) *Soldiers, Peasants, and Bureaucrats: civil–military relations in communist and modernizing societie*s, George Allen & Unwin, 1992, pp. 9–27.

[13]Ibrahim El HOUDAIBY, *Fighting the last war? Civil-military relations in Egypt*, Fride – Policy Brief, April 2014

[14]Stephanie CRONIN, *Armies and State Building in the Modern Middle East: Politics, Nationalism and Military Reform*, I.B.Tauris, 2013.

identities or has contributed to the changing processes of perverted regimes. Furthermore, military leaders have often exceeded the limits of their institutional status and, implicitly, exceeded official constitutional principles to substitute civil political forces that are an essential element for any real democratic system; here also, the army becomes an *asabiyya*, a solidarity network which takes over the authority and resources of the state on behalf of a particular elite. The dialectics and rivalries for power between civilians and army are found in almost all republican regimes in the Middle East and are a structural part of the political culture here. In the present monarchist regimes, with a large democratic deficit, the army, even if loyal and closely connected to the privileges of power, can go towards two extremes, either to challenge or undermine the political powers or, on contrary, to try pressure for democratization and liberalization of the political and social space.

3. Religion: tool or threat for democratic transitions?

Probably, the most debated and controversial relationship when dealing with the Arab-Muslim World is that between religion, portrayed by Islam, and democracy[15]. It is the theme that focuses on a broad range of collective stereotypes and misunderstandings of the complex particular situations concerning weight attached to Muslim values and rule that structure behavior and define the political context of countries from the region. Within this framework, differences are taking the shape of historical background, of religious and cultural traditions; the assuming phenomenology, individual and collective, of Muslim identity and rules have an endless variety. In this case, democratization theories regarding the Middle East cannot be elaborated without taking into consideration the increasing importance of Muslim references in shaping the scenarios and democratization projects, especially in the context of post-2011 mutations. We must, first of all, accept the multiplicity of viable options for state-religion relationship in contemporary societies. The image, once a traditional pattern, built upon Western modernity tributary to secularization ideas, which conditions the existence of democratic societies to ensure a secular public space, placing into brackets the religious and identity references, is today outdated[16]. Even in Europe, the relationship between democracy and religion is far more complex and there are countries such as Germany, Belgium, The Netherlands and Switzerland, where the state harnesses in an official manner the role of religion as an important agent for building a democratic space and the Churches are involved in supporting the social integration of their citizen's behavior. In states such as Denmark, Sweden, Norway, the United Kingdom, there are national Churches and here the national identities are deeply connected to the confessional one, even if, at an individual level, the existential assumption of Christian values is rather moderate, due to an accelerated secularization. Consequentlly, some perspectives accept that religion can and must be assessed as an agent in reshaping the values and practices of democracy – is what took the name of „twin tolerations" - between state and religion[17]. Like there are „multiple secularizations" there are also multiple re-*enchantments,* recovery dynamics to religion that reconfirm, in post secular societies, the presence of religion as an existential balance source and axiological reference.

---

[15]John ESPOSITO*, Islam and Democracy*, Oxford University Press, 1996.
[16]Veit BADER, *Secularism or Democracy? Associational Governance of Religious Diversity*, Amsterdam University Press, 2014.
[17]Alfred STEPAN, „Religion, Democracy, and the "Twin Tolerations", *Journal of Democracy*, Vol. 11, No. 4, 2000, pp. 37-57.

The Islam is here a classical example, especially because it has the structural vocation of being an integrated normative support, altogether *Dīn-Dunya-Dawla* (religion-world-state). Once with the modern times, many representatives of Muslim community, from within or outside, tended to blame it on what they considered a persistence of cultural inheritance, and Muslim socio-politics, seen as an agent that delayed modernizing process of Muslim societies and the assumption of a democratic pattern, like in European historical tradition, separation of the state from Church and from Christian political values. This offered the chance of building modern philosophy and modern political praxis, based on individual valorization and of its freedom. Even if there is governance and specific political patterns, in Muslim traditions regarding the state and the status of its citizens within society, the Islam cannot be perceived as antidemocratic by nature.

Particularly, the new Islamist ideologists following Rashid Rida and, more recently, Tariq Ramadan or Rachid Ghannouchi, theorize largely about concepts, values and democratic practices that structurally pertain to the Islamic tradition. This is mostly about the classical principle of "consultation" (*shūrā*), seen as an archaic democracy form of Muslim kind[18]. At the same time, following the nineteenth century, a significant number of states from the Arab – Muslim World have replaced the traditional social, political, and juridical norms and values with new values, practices, and codes they took from the modern West, apart some exceptions, like the conservative monarchies (first of all Saudi Arabia) and certain other regimes, which programmatically aim at a new Islamization of the political, social, and juridical domains (like the Republic of Iran, or Pakistan during Zia-ul-Haq)[19]. Thus, the real factor that blocks democratization process is not actually religion, but rather the diverse radical and authoritarian interpretations religion receives. Such interpretations serve the "secular" authoritarian practices certain political regimes from other countries would follow. Actually, desiring to legitimize their positions, many authoritarian regimes tried to confiscate and use the Muslim discourse and religious themes in their own advantage. They attempted to borrow the authority of Islam, in order to gain adhesion of the masses.

Consequently, the central role that Muslim religious references play in the lives of believers turns this aspect into an unavoidable factor one needs to consider when discussing democratic optimization of the Middle East. The process of secularization does not necessarily lead to great democracy. The problem with Islam is that, lacking a unique magisterium and a clear univocal dogma, it constantly lends itself to different interpretations, in accordance with the interests of agents who take upon themselves the role of speaking in its name. The widespread emergence of Islamic ideologies and currents that plead for conservative models concerning the structure of justice, society, and politics, often imposed by force, led to numerous debates in the last decades, about the distance that exists between such projects and classical ideals of Western democracy. Thus, for instance, since the seventies two important schools of thought developed among scholars, their conclusions often influencing the decisional process. For some (Bernard Lewis, Fouad Ajami, Samuel Huntington), Islam is structurally incompatible with modernity and democracy, therefore, in order to create a democratizing dynamic in the Muslim World, one needs to act from outside[20]. The neoconservative geopolitical view, in which originated the idea to initiate actions in Afghanistan and particularly Iraq, has emerged, since 2001, assuming this line of

---

[18]Fahti OSMAN, *Islam in a Modern State: Democracy and the Concept of Shura*, Center for Muslim-Christian Understanding, Georgetown University.
[19]Nader HASHEMI, *Islam, Secularism, and Liberal Democracy: Toward a Democratic Theory for Muslim Societies*, Oxford University Press, 2012.
[20]Bernard LEWIS, „Islam and Liberal Democracy: A Historical Overview", *Journal of Democracy*, Vol. 7, No. 2, 1996, pp. 52-63.

thought. For others, however, neither Islam, nor political Islam or Islamism (with the exception of its radical forms) is antidemocratic. Moreover, they say, the Islamic forces and even political Islam, like the Muslim Brotherhood, are potential agents for the internal destructuring of authoritarian systems, being able to act as vectors of possible democratic openings in the practical sense (parties, elections, and the implementation of a real autonomy for state institutions)[21].

Since 2011, all mentioned models had the opportunity to be tested with respect to their real validity and limits. During the Arab revolutions of that period, Islam seemed to be an essential and significant animating factor for protests and expectations, for both the elite and masses. The elections that followed (Tunisia, Libya, and Egypt) have confirmed through the ballot box what the people expected from Muslim values and from the political parties that took upon themselves to defend and implement a Muslim vision of society and politics. However, those popular expectations did not necessarily emerge from the people's desire to transform Islam into an ideological and normative support. It rather sprang from the fact that, by its very nature, Islam pleaded for the ideas of justice, social and economic equity, and for the need to have politics maintaining a certain sense of reverence toward the interests of community. Egypt is here the main example. Thus, one should not explain the success of the Muslim Brotherhood and Salafi parties in 2012 in terms of their electoral basis, but rather in popular understanding terms of the Islamic ideals. In the post-revolutionary Arab states (as well as previously in Turkey, Morocco, Algeria, Indonesia, Palestinian territories etc.), the democratic legitimization of Islamic parties was a sign of the symbiosis that could exists between need and the desire for democracy in politics and the fact that Muslim themes can serve as motive force and ideological support for the implementation of democratic behavior[22]. Obviously, there are numerous radical interpretations of the Islamic tradition, such as interpretations of Salafi-jihadism; they anathematize the theoretical and practical system of democracy as heresy and foreign innovation (*bi'da*). They also plead for the establishment of new totalitarianism, in the name of an absolute and exclusive Islam, which they interpret in ways that radically modify its classical meanings, such as defending the individual and constructing a state and a society open to otherness. Thus, religion can have a double role. It can become either a doctrinal basis for new political and social authoritarianism, as in Taliban period or even the Saudi Kingdom, or, on the contrary, it can become a "liberation theology" - the means of freeing social and political spheres from the totalitarian pressure created by different exclusivist groups and it can help people become aware of the central role of individual, both religiously and socio-politically.

Obviously, today we see a great number of perils and deformed attempts to assume the Muslim identity and behavior. They have an impact upon the capacity of certain societies and states to implement democracy. First, this is about the widespread and particularly violent resurrection of communitarianisms in Iraq, Syria, Lebanon, and the Gulf area, where group identities become more important than their collective condition as defined by modernity, national membership, and even by the fact that they share same religion. Current tensions between Sunni and Shi'a affect the capacity for democracy of states like Iraq, Lebanon and Pakistan. Similarly, the violent cohabitation of hundreds of radical groups, in the conflict zones of Syria, Libya, Iraq or Afghanistan, undermines security, social pacification and the establishment of democratic institutions and practices. Thus, one can safely say that Islam

---

[21]John ESPOSITO, François BURGAT (eds.), *Modernizing Islam: Religion in the Public Sphere in Europe and the Middle East*, Rutgers University Press, 2003.
[22]Adeed DAWISHA, *The Second Arab Awakening: Revolution, Democracy, and the Islamist Challenge from Tunis to Damascus*, W.W. Norton, 2013.

itself does not represent a danger for democracy, the danger comes from the aberrant confiscations of Islam, which distort its true significance and vocation. Even in the case in which it proposes social, political, or juridical models taken from its own doctrinal resources and from specific Muslim traditions, there can appear social and political structures able to assimilate classical democratic values, as they are today in universal and normative form[23]. Of this kind is, for instance, the model that the new generations of Islamists increasingly employ, from Tunisia to Syria. This model pleads for a natural integration of religious ideas with certain democratic systems, replacing a "secular" state (like those in the West), or a religious theocratic state (like the Iranian Republic, or even the binary Wahhabi-Saudi model) with a "civil state" (*dawla madaniyya*), in which democratic values, institutions, and practices coexist with Muslim values in the public space[24].

Conclusions

Nowadays, the Middle East and North African region seems to continuously remain inconsistent regarding the capacity to realize an effective transition towards a real democratization of political practices and governance models. The current political-military crises, which have succeeded 2011 events, demonstrate the fragility of states and their societies, the difficulty of legitimizing democratic norms and making them functional, despite the formal instauration of institutions and election practices taken from Western democratic models. As in post-revolutionary situations of Libya, Egypt, Yemen and even Tunisia, as well as post-Saddam Iraq prove it, what produces a democratic deficit is the incapacity of systems to attenuate their authoritarian conditioning, the state-society polarization, internal fragmentation and persistence of cultural and socio-political models much too tributary to other values than those which found liberal democracy. Finally, in the actual context of political and security instability and even a raise in fragmentation of the state order in several countries from the region, issues of accepting or even facilitating, from pragmatic considerations, the instauration of hybrid regimes are raised more and more, hybrids in which Western type democratic institutions would coexist with practices that are stemmed by the specific traditions of local political culture.

Acknowledgement:

This work was possible with the financial support of the Sectoral Operational Programme for Human Resources Development 2007-2013, co-financed by the European Social Fund, under the project number POSDRU/159/1.5/S/138822 with the title ***"Transnational network of integrated management of intelligent doctoral and postdoctoral research in the fields of Military Science, Security and Intelligence, Public order and National Security – Continuous formation programme for elite researchers - "SmartSPODAS"."***

BIBLIOGRAPHY:

1. ALATAS Syed Farid, "Ibn Khaldun and Contemporary Sociology", *International Sociology*, Vol. 21, No. 6, 2006, pp. 782-795.
2. BADER Veit, *Secularism or Democracy? Associational Governance of Religious Diversity*, Amsterdam University Press, 2014.

---

[23] Judith COCHRAN, *Democracy in the Middle East: The Impact of Religion and Education*, Lexington Books, 2013.
[24]Peter HILL, „"The Civil" and "the Secular" in Contemporary Arab Politics", *Muftah*, February 26, 2013.

3. CHRISTIE Kenneth, Mohammad Masad (eds.), *State Formation and Identity in the Middle East and North Africa*, Palgrave Macmillan, 2013.
4. COCHRAN Judith, *Democracy in the Middle East: The Impact of Religion and Education*, Lexington Books, 2013.
5. COOK Steven, *Ruling But Not Governing: The Military and Political Development in Egypt, Algeria, and Turkey*, Council on Foreign Relations, 2007, pp. 93-132.
6. CRONIN Stephanie, "The Army, Civil Society and the State in Iran: 1921-26", Touraj Atabaki, Erik Zurcher (eds.), *Men of Order: Authoritarian Modernization Under Ataturk and Reza Shah*, I.B.Tauris, 2004, pp. 130-163.
7. CRONIN Stephanie, *Armies and State Building in the Modern Middle East: Politics, Nationalism and Military Reform*, I.B.Tauris, 2013.
8. DAWISHA Adeed, *The Second Arab Awakening: Revolution, Democracy, and the Islamist Challenge from Tunis to Damascus*, W.W. Norton, 2013.
9. DIAMINT Rut, BARAH Mikail, *Militaries, civilians and democracy in the Arab World*, Fride – Policy Brief, January 2012.
10. DIAMOND Larry, Marc Plattner (eds.), *Democratization and Authoritarianism in the Arab World*, Johns Hopkins University Press, 2014.
11. EL HOUDAIBY Ibrahim, *Fighting the last war? Civil-military relations in Egypt*, Fride – Policy Brief, April 2014.
12. ESPOSITO John, François Burgat (eds.), *Modernizing Islam: Religion in the Public Sphere in Europe and the Middle East*, Rutgers University Press, 2003.
13. ESPOSITO John, *Islam and Democracy*, Oxford University Press, 1996.
14. FUAD Khuri, *The Study of Civil Military Relations in Modernizing Societies in the Middle East: A Critical Assessment*, UCLA Center for International and Strategic Affairs, 1982.
15. HASHEMI Nader, *Islam, Secularism, and Liberal Democracy: Toward a Democratic Theory for Muslim Societies*, Oxford University Press, 2012.
16. HILL Peter, "The Civil" and "the Secular" in Contemporary Arab Politics", *Muftah*, February 26, 2013.
17. KHURI F.I., "The study of civil–military relations in modernizing societies in the Middle East: a critical assessment", in R. Kolkowicz, A. Korbonski (eds.) *Soldiers, Peasants, and Bureaucrats: civil–military relations in communist and modernizing societie*s, George Allen & Unwin, 1992, pp. 9–27.
18. LEWIS Bernard, "Islam and Liberal Democracy: A Historical Overview", *Journal of Democracy*, Vol. 7, No. 2, 1996, pp. 52-63.
19. LEWIS Bernard, *What Went Wrong? The Clash Between Islam and Modernity in the Middle East*, Harper Perennial, 2003.
20. OSMAN Fahti, *Islam in a Modern State: Democracy and the Concept of Shura*, Center for Muslim-Christian Understanding, Georgetown University.
21. OWEN Roger, "State and Society in the Middle East", in Philip S. Khoury, Joseph Kostiner, *Tribes and State Formation in the Middle East*, University of California Press, 1990.
22. PICARD Elisabeth, "Arab military in politics: From the revolutionary plot to the authoritarian state", in Giacomo Luciani (ed.), *The Arab State*, University of California Press, 1990, pp. 189-219.
23. PION-BERLIN David (ed.), *Civil-Military Relations in Latin America: New Analytical Perspectives*, The University of North Carolina Press, 2000.
24. ALFRED Stepan, "Religion, Democracy, and the "Twin Tolerations", *Journal of Democracy*, Vol. 11, No. 4, 2000, pp. 37-57.

THE PSYCHOLOGICAL THEORY OF SUICIDE - SUICIDAL TYPOLOGIES IN TERRORISM

Anghel ANDREESCU
Questor General of Police (R), PhD professor with "Carol I" National Defence University, Bucharest, Romania

Raluca COŞEA
Assistant Researcher, PhD candidate with "Carol I" National Defence University.
E-mail address: raluca_cosea@yahoo.com

Abstract: *Suicide is a subject that has caused wonder and repulsion over time in all cultures and civilizations across the globe. Quran dictates his followers that suicide is forbidden - "Do not kill yourself.", and considered in the collection of anecdotes of Prophet Mohammed as prohibited. Suicidal missions became known worldwide after the Japanese kamikaze practice, practice that turned overnight into martyrdom.*

Terrorist leaders manipulate followers to take life without feelings of regret. Suicide is an act of free will, a person's freedom to dispose of his body at any time. From an ethical point of view, the history describes suicide as an act of cowardice that comes from disappointment with life. Social implications of multiple and diverse consequences that lead to the implementation of this act so much contested, brought this concept and this fact to the attention of sociologists, psychologists, philosophers, and especially that of theologians and church, whether Orthodox or Catholic.

The purpose of this study is to focus attention on the types of individuals and groups that have tendencies towarss terrorism. More over, the study examines the current knowledge of the subject and the types of suicide and tries to develop psychological and sociological profiles of terrorist individuals, trends, motivations, behavior and vulnerabilities.

Keywords: *suicide, kamikaze, terrorism, manipulation, psychology, sociology;*

1. Why good people turn evil?

The mind is its own place, and in itself can make a heaven of hell, a hell of heaven.
- John Milton*, Paradise Lost, 1667*

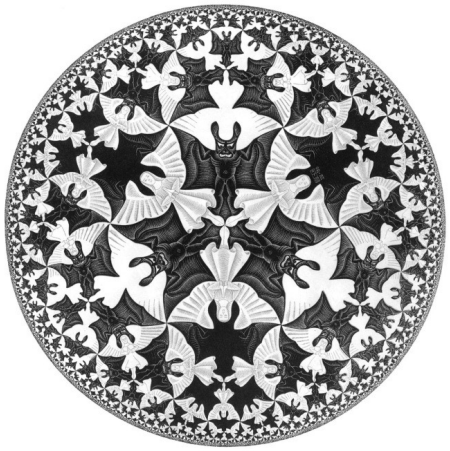
Every individual and every group has a specific tendency towards suicide, tendency that cannot be explained neither through the person's physic or constitution, nor by the individual's nature or by the environment in which that person lives. However, in the case of a person borne, raised and grown up in a deficient society, morally speaking, those factors that can convince the individual to think of suicide can be more complex, than in the case of a normal society, without important social or moral *earthquakes*. This cannot be a strict rule, but that tendency towards suicide is without a doubt linked to social grounds, constituting itself as a collective phenomenon.[1]

Terrorist organizations are considered closed societies, in which leaders welcome persons with different personalities, people with an extremely high IQ, professionals in their domain, researchers, scientists, but also people whose sole purpose in life is revenge. It is

[1] Emile, DURKHEIM, *Despre Sinucidere*, Institutul European, Iaşi, 2007, p.133.

obvious that we cannot compare people with lab rats, but, not once they have given us proofs of similar characteristics and they are treated, manipulated and sacrificed like guinea pigs, as the sole wish of their master or leader. These closed societies, the terrorist organization can offer to their followers the possibility of refusing these types of offers.[2] As Eric Berne explaines in *The Psyhology of Human Destiny* the fact that "...the cage has an open door and the individual just needs to get out if he really wants. If he doesn't want to get out, most of the times his own senaryo (the way he draw his own destiny) is the one that keeps him stranded. That cage is a cosy and familiar place"[3].

The concept of evil can be best described by M.C.Echer's "Circle Limit IV" *(Image no.1, Circle Limit IV)*[4].



His periodic drawing division has been the most popular of his work, which is related to the mathematical concept of tessellation of the plane. Echer mentioned that: "it is the richest source of inspiration that I have ever tapped, and it has by no means dried up yet".[5] The image describes the world with both good and evil, and the barrier between those two is very penetrable and imprecise. The most important characteristic is that it is possible that those angels become devils and vice versa? Can good people become evil? And if yes, how is that possible? These are the most important questions in Philip Zimbardo's book *The Lucifer Effect*.

The ultimate transformation of good into evil is that of Lucifer "the light bearer"[6] into Satan. After he challenged God's authority he was send into Hell, along with other fallen angels. In Milton's *Paradise Lost*, Satan claims that is "better to reign in Hell than serve in Heaven"[7].

We all fear evil, but at the same time, we are fascinated by it, explaines Zimbardo and at the same time tries to understand and explain the processes of transformation from good to evil: "…too often we look to the stars through the thick lens of personal invulnerability when we sould also look down to the slippery slope beneath our feet"[8].

Evil is perceived as an entity, a characteristic that some people inherit and some do not. It is considered that if you have something bad since childhood, as your destiny unfolds, you will become bad wheather you want or not. Evil is defined by looking to history's bad leaders as Stalin, Hitler, Pol Pot, Idi Amin, Saddam Hussein, and others who ordered mass murders. This type of evil is extreme, but evil are also considered, rapists, drug dealers, perpetrators, bullies, terrorists, etc.

In the case of follower, in a terrorist organization, he can rememorate his life and understand that if his society showed no signs of acceptance and understanding, that it didn's provide his psychological needs, this opportunity is now offered to by the terrorist leader and his new society. It is certainly a chance given to him, hidden in a simpler or more complex form of manipulation.

The individual observes the outer world with good and with bad things, which on some level scares him. Thus, unable to cope with daily stress, returns to a broken society where he is gladly received. Accepting such an offer comes with joy and gratitude. He will be

---

[2] Eric, BERNE, *Ce spui după Bună Ziua? Psihologia destinului uman,* Editura Trei, București, 2006, pp.90-94.
[3] *Ibidem.*
[4] http://www.wikiart.org/en/m-c-escher/circle-limit-iv - Accessed at 13.09.2014.
[5] http://www.math.cornell.edu/~mec/Winter2009/Mihai/section8.html/ - Accesed at 08.09.2014.
[6] Philip, ZIMBARDO, *The Lucifer Effect – How good people turn evil*, Random House, U.K., 2007, p.3.
[7] *Ibidem.*
[8] *Idem*, p.5.

given only appreciation, so long as he does as he is told. He will then be free in that new society as Berne's guineea pigs "...man returns to his cage filled with buttons and pedals, knowing that if he does his work, and push on the right ones, he will be given food, drink and one thrilling occasional experience"[9], as in the case of suicide bombers, the follower will return for the final experience that will take him to paradise.

This society's terrorist leader provides a transparency of thoughts and of his plans, wanting his followers's feeling of trust to be directly proportional to their desire to help and agree with the organization's strategies and requirements. And yet, more often the motivations of a terrorist attack and its details are not shared among all members, thus risking to be caught or killed by the forces fighting against them. Another drawback that can occur following a loss of information is the emergence of dissension among those who deal directly with such attacks. That is why a divided group or organization is not their wish and it is not desired in their *society.*[10]

In the chapter "Crimes against Humanity: Genocide, Rape and Terror", Zimbardo explaines us the fact that is time after three thousand years, to understand that *no person or state is incapable of evil*[11]. History mentions Agamemnon's desire to kill all of his enemies that had the courage to confront him: "We are not going to leave a single one of (the Trojans) alive, down to the babies in their mothers' wombs – not even they must live. The whole people must be wipped out of existence…"[12] This is why we live in the *mass murder*[13] *century*, and the same words of Agamemnon where used by leaders of Hutus, in the African nation of Rwanda, before the Tutsi minority was wipped from the face of the world: "*We are going to kill all the Tutsi, and one day Hutu children will have to ask what a Tutsi child looked like".*[14]

As President Franklin Roosevelt said: "*Men are not prisoners of fate, but only prisoners of their own minds"*[15]. And the best metaphore for this statement compares contraints and loss of mind freedom with real prisons, a concept from which Phillip Zimbardo started his *Standford Prison Experiment*, wanting to understand evil and its ways.

2. Theory of suicide

We're all guinea pigs in the laboratory of God…
Humanity is just a work in progress.
- Tennessee Williams, *Camino Real* (1953)

Suicide is a global issue that provoked repulsion and astonishment over time in all cultures and civilizations. The Quran dictates its adepts that suicide is *haraam*, meaning strictly forbidden. Suicide actions started in history as individual missions. The Japanese kamikaze became martyrs and heroes overnight, for their families and most important of all, for their society.

[9] Philip, ZIMBARDO, 2007, *op. cit*., p. 5.
[10] Sorin, TOPOR *O scurtă istorie a terorismului*, Editura Universităţii Naţionale de Apărare „Carol I", Bucureşti, 2013, p. 159.
[11] Philip, ZIMBARDO, 2007, *op. cit*., p.12.
[12] *Ibidem.*
[13] *Idem*, p.15 – The opinion of Alison des Forges of Human Rights Watch who has been researching many mass murders and extreme crimes: *This behavior lies just under the surface of any of us. The simplified accounts of genocide allow distance between us and the perpetrators of genocide. They are so evil we couldn't ever see ourselves doing the same thing. But if you consider the terrible pressure under which people were operating, then you automatically reassert their humanity – and that becomes alarming. You are forced to look at the situation and say, „What would I have done? Sometimes the answer is not encouraging."*
[14] *Idem*, p. 15.
[15] *Idem*, p.21.

Back in history the samurais used to kill themselves to honor their Lord, and the kamikazes in honor of the Emperor. The difference between these two is that kamikaze is the attack on the enemy by killing oneself, but in the case of a samurai, the typical case is hara-kiri, that does not include the element of attack at the same time. Both samurais and kamikaze individuals offer the utmost expression of their will and desire to become true heroes and die as martyrs.[16] As a proof of their way of thinking and contentment in dying for their lord or for their Emperor, on the 28th of October 1944, is Isao Matsuo who wrote a letter to his parents explaining why his mission will make his a martyr and a hero:

"Dear Parents:

Please congratulate me. I have been given a splendid opportunity to die. This is my last day. The destiny of our homeland hinges on the decisive battle in the seas to the south where I shall fall like a blossom from a radiant cherry tree. I shall be a shield for His Majesty and die cleanly along with my squadron leader and other friends. I wish that I could be born seven times, each time to smite the enemy.

How I appreciate this chance to die like a man! I am grateful from the depths of my heart to the parents who have reared me with their constant prayers and tender love. And I am grateful as well to my squadron leader and superior officers who have looked after me as if I were their own son and given me such careful training.(...)

I hope that my present deed will in some small way repay what you have done for me. Think well of me and know that your Isao died for our country. This is my last wish, and there is nothing else that I desire. I shall return in spirit and look forward to your visit at the Yasukuni Shrine.(...) We are 16 warriors manning the bombers. May our death be as sudden and clean as the shattering of crystal."[17]

In what concerns terrorists, more than once, their thoughts on martyrdom and becoming a hero for their leaders or country, highly assembles with Japanese concepts. Without trying to make a connection between the concept of suicide, terrorism, manipulation and the power of a terrorist leader to convince his adepts to take their life without regrets, suicide is an act of free will, someone's right and liberty to dispose of one's body at any time.

Multiple social implications and numerous consequences that lead to this type of attack, brought this concept and reality to the strict attention of sociologists, psychologists, philosophers, but most of all to theologians and religious formations, orthodox, catholic or Muslim. Pierre Moron, researcher on suicide, in his book, *Le Suicide* explains the fact that *"Suicidal thoughts, mere mental representation of this act, have to be virtually excluded from the study on suicidal behavior which, by definition, begins with the action itself. Considering it virtual, means to mentally represent the same instinctive emotional impulses that arise with the act itself: the intention of killing self."*[18]

Psychologically speaking, the vast majority of terrorists are not psychotic, as it was believed until now. Also, they do not suffer of psychiatric disorders; on the contrary, they are rational individuals, dedicated to a *noble* cause, from their point of view. The terrorist does not conceive and understand his or her victim's sufferings. Instead, the leader of such groups has intelligence above average and is capable to estimate the costs and especially the earnings of such attacks.

Their personality and being extremely sociable, helps them to draw countless disciples that will surely be convinced that the goals of the organization are in the forefront. The leader is a charismatic individual, charisma that will be an advantage in convincing those around him that all actions that the group will organize in the future are correct and joining the terrorist organization is necessary for carrying out its purposes.

---

[16] http://www.isc.meiji.ac.jp/~takane/academy/kamikaze/kamikaze-sie.htm - Accesed at 06.09.2014.
[17] http://www.geocities.jp/kamikazes_site_e/isyo/isyobun/matsuoisaoisyo.html - Accesed at 06.09.2014.
[18] Jean, AMERY, *Despre Sinucidere: Discurs asupra morţii liber alese*, Editura ART, Bucureşti, 2012.

Religious leaders often resort to religious quotes to justify their crimes and violence, in order to carry out the goals, even if they are religious, financial or political. Terrorist groups offer to their members a sense of belonging, a sense of power and in some cases the need for revenge after the death of a family member. In such organizations, discrediting and diminishing the leader's power may be the best way to shatter the group, to divide their adepts and new recruitment can be stopped.

In the case of terrorism, the individual, group and organization are interdependent, so they are mutually reinforcing. To achieve their objectives, the organization is based on what individuals in the group undertake. The organization works subtle with individual's psychology. Optimal functioning of a terrorist organization requires the adept willingness to contribute and engage in activities designed and implemented by the leader of the group. The availability of a devotee comes from amplifying the actions of socialization and indoctrination in the group of individuals. Self-sacrifice, the sacrifice of life is not an adaptive trend and unfortunately there are many people agreeing with such deeds, giving the promise that they will become martyrs and heroes of their societies.[19]

The character traits are the main features by which the leader chooses its followers, so he will then be able to fully engage in and act according to the wishes of the leader. Sageman, in his book, *Understanding Terror Networks*, notes that: *...are usually completely normal people...ordinary people like you and me. In many respects they are among the brightest in the societies from which they come."*[20] Whatever the social background of the individual is, the vast majority of terrorists define their own identity with that of the community, group or leader. The objectives of the terrorist leader are to persuade its followers, which in turn are required to determine their society or even the world, to see life as they see it.[21]

In 1805, presbyterian priest Samuel Miller described suicide as *"...the most sordid selfishness and unworthy impulse. It is a crime that sacrifices everything on the altar of personal feelings."*[22] Thinking of suicide as a selfish act can be understood in the sense that people still are convinced that those who have committed suicide did not think for a moment at the impact of their deaths on their loved ones or on their society. The impact of a terrorists death in his own view, is a positive and not a negative one. The act itself, the death of other people with him, is seen as a blessing that Allah gave him. The suicide bomber seeks a well established plan, accepts manipulation by its leader and rarely the suicide bomber has hard moments in terms of consequence and fatal outcome of his actions.

3. Manipulation and obedience

It is when power is wedded to chronic fear that it becomes formidable.
- Eric Hoffer*, The Passionate State of Mind, 1997*

Psychological manipulation is characterized as everything being primarily focused on the influence of psychological processes and phenomena of the manipulated person, processes that are involved in structuring, guiding and supporting attitude and behavioral system of the target. These processes can be found in the sphere of perception, social representation, thinking, affectivity, motivation, etc. A series of physical phenomena from the emotional, cognitive and relational system can be used by the manipulator, with excellent results in the

[19] Kenneth C. RUGE, Barry, LENSON, *Sindromul Othello*, Curtea Veche Publishing, Bucureşti, 2012, p.60.
[20] Marc, SAGEMAN, *Understanding Terror Networks*, University of Pennsylvania Publishing, U.S.A., p45.
[21] Raluca, COŞEA, *Psihopatologia Teroristului Sinucigaş*, Timpolis Newspaper, 18-23 aprilie 2013, Online edition.
[22] Thomas, JOINER, *Mituri despre sinucidere*, Editura Trei, Bucureşti, 2013, pp.40-52.

determination and control of human behavior, especially when this method is combined also with the influencing of information.

The terrorist leader is an exquisite psychologist in most of the cases. He is also an individual who recognizes his most important strengths in terms of conviction, charisma and especially manipulation, implemented to achieve political, military, economic or revenge goals. The leader must understand each individual from the group or organization, using a proper methods of speech, verbal and nonverbal, for the effective management of individuals and of the organization overall, thus being able to work optimally.

Among the most important qualities of a terrorist leader, although there isn't a common point, a core of features that give us assurance that the person will become a leader, we can observe: above average intelligence, aggression in thought, but also patience and the motivation to carry out any purposes he established. Other characteristics can be extreme ambition, self-confidence, a manipulator character, and why not, lack of compassion for those who will die or died in the terrorist attacks, followers or other innocent people. Undoubtedly, these qualities are necessary, but by no means sufficient, because the situations that the leader may face are specific and diverse, so the personality of the leader will have to mold onto the organizations or the follower's character, but certainly this will have to be bilateral[23].

The personalities and characteristics of those individuals who accede to a place in such an organization and the efficiency features are very important. The terrorist frontrunner will attract people who have the urgent desire for revenge, those who want be part of a group, a society, those who need to be loved and love, need to be part of a reference group that accepts you and will make them feel wanted.

Relying of such *gifts*, the terrorist organization gives individuals that serenity, a life in an orderly, stable and predictable world, with respect and status that the other group would have never given. Special techniques are used to trigger manipulative actions, guidance and control techniques psychic processes and phenomena, so that the target will correspond to the interests of the leader.

Among the many processes and phenomena the most significant are: the tendency toward cognitive and emotional balance, cognitive dissonance, social comparison, the effect of priming, snap and that related to psychological commitment. Furthermore we can see Oedip's phenomenon, fear, the positive effects of reward on individual options, the ascendency of the group to its members, the halo effect and the charisma effect, the phenomenon of controlled suggestion, role play etc.[24]

Those phenomena mentioned above are used as a powerful tool for manipulation, so that the target perceives it as an imbalance in cognitive or emotional level. Functional features of dissonant situations uses these phenomena in manipulative actions: thus, they artificially induce dissonant elements in relevance to a certain attitude that is intended to be changed in the future, so as to obtain a spontaneous change in the structure or method of its objectification, for the manipulator's purpose, a subtle action, where the effect is obtained through rebound.

Totally unique manipulative possibilities are also offered by Oedipus syndrome or phenomenon – occurrence that designates the trends of a prediction just because the predictions were made. The result of such actions, like psychosocial phenomena that underpin some guidelines and the declaration of plans already accomplished, are current ways of manipulation.

Another method of manipulation which is recurrent in the case of terrorist groups and organizations, is the act of inducing fear, along with a *gift* from the leader, that being the offer

[23] http://psihologia.sinners.ro/2010/02/24/caracteristicile-unui-lider-eficient/ - Accesed on 06.10.2013.
[24] http://www.despresuflet.ro/forum/comunicare-f40/manipularea-mecanism-de-realizare-a-influentei-t487.html - Accesed on 06.10. 2013.

of a saving solution. In this case, fear is a powerful influence on individual behavior, especially if the leader is evil enough to provide also the solution for avoiding or escaping from a specific situation. It can promote interpretations that suggest serious dangers to the individual, group or community and the solution for preventing these is contingent on the manipulator's interests.

Some of the most popular direct manipulation techniques are based on the phenomena and effects mentioned above and they are used in different circumstances, with various objectives, ranging from the commercial to the political ones.

Social situations exert significant control over human behavior. Individual's actions and reactions to stimuli of a particular social environment are determined by specific forces and constraints in a specific environment, to a far greater extent than would be expected if only the intimate personality of that person would be concerned.

The manipulation analysis, explained to all people, is meant to warn the individual about the pressures that determines one's behavior and way of thinking, but mostly it may give beneficial solutions for crisis situations.

4. Suicidal typologies

Every act of suicide needs and has specific characteristic that helps that act to exist and happen. According to psychologist Emile Durkheim, after the cause that triggers it, there are four types of suicide: *egoistic, altruistic, anomic* and *fatalistic*.

4.1 Egoistic Suicide

The European map of suicide shows us that in Catholic countries like Italy, Spain, Portugal, the suicide rate is low, however protestant countries have one of the highest rates of suicide, as in Saxony and Denmark. The result of this research is that inequality of culture can be the real cause of the discrepancy between Catholic and Protestant religion.

Most terrorists purpose is to accede to *paradise*, which in case of Islam, has a strong religious characteristic. The idea of approaching Allah and that contentment offered by the leader to the individual who accepts death, can be characterized without any doubt as *selfish suicide, egoistic suicide*. This type of suicide occurs where excessive individualism and a low level of social assimilation, it refferes to people not being members in a social group, and those will appeal to suicide.

When the individual chooses to detache himself from his society, without noticing, he or she will automatically detache from life. The need of a future bomber to fight against all, to fight against a normal or abnormal society, is extreme. He or she is unable to communicate freely with the rest of the population, the result being the deterioration of social and familial bonds, and the deterioration of him or her as a human being.

A society with high integration, will give to its individuals high value in human existence. On the contrary, low values in a society with low integration, will trigger a higher suicide rate. An additional element that best describes the reason of suicide is a broken social environment where life is only seen in grey and black, and improvement has no place in there. According to Emile Durkheim, the person who commits egoistic suicide is "*characterized by deep meditation and self-examination, while the self of the person committing anomic suicide is marked with keen desire and sensuality"*[25].

Durkheim bind egoistic suicide with deterioration and the anomic suicide is linked to disillusionment and disappointment. In his opinion, the most important typologies are egoistic

[25] http://sociologyindex.com/egoistic_suicide.htm - Accesed at 11.09.2014

and anomic and the reason why people kill themselves is because *"there is a specific tendency to suicide [that depends] upon social causes..."*[26]

In a group or organization, people can have a higher or a lower level of attachment to that group. The concept of attachment is synonymous with social integration. Atypically high or low levels of social integration may result in suicide acts. At the same time, low levels have the same effect because it causes people to turn to suicide as a last option.

Furthermore, Durkheim explaines that suicide rates are higher for single, divorced or widowed people than for those who are married, because marriage improves the sense of belonging, this making the seperation difficult. Egoistic suicide is described by the victim's failure to resolve his or hers life dilemmas.

In times when society is disturbed and anxious, ruffled by a high intensity crises or on the contrary an extremely happy moment, that came suddenly, the action exert by society is temporarily stopped. The result of these shutdowns is the sudden uplifts of the number of suicides.

4.2 Altruistic Suicide

Emile Durkheim used the concept of "altruism" to describe a suicide dedicated for others or for the community. This includes kamikaze, the self-sacrifice for military objectives in wartime. Suicides of this type reflect courage and indifference for the loss of others life. Altruism is a

Altruism is a social behaviour that is described as someone's interest in the wellbeing and welfare of other individuals, members of groups or the organization as a whole. The principle of action is the altruistic regard for others.

Durkheim specifies that, *„In life, everything must be in balance. A biological nature can not fulfill its mission unless it has certain limits. This observation also applies to social phenomena. (...) When one is isolated from society, it's easier to take his life, but he will also do that when he is too integrated in that society"*.[27]

The word altruism expresses quite well the opposite state of selfishness, that condition in which the ego that does not belong to itself and its tangled with something from the outside. The pole of that conduct belongs to that group. When we look at the idea of altruistic suicide, Durkheim explained that there are two types of altruistic suicide, the *simple altruistic suicide* which is the result of a simple intense altruism and *obligatory altruistic suicide* that is committed as a duty, just as in most cases of suicidal terrorism. Such a division is necessary because not every altruistic suicide can be defined as mandatory, sometimes being considered optional.

In the new contemporary society, as individual personality is increasingly let free from collective personality, altruistic suicide type simply are not that common. Some soldiers prefer death instead of humiliation if defeated, as were Beaurepair, Admiral Villeneuve or samurais, and those who committed suicide to protect their families from shame. All of them surrender to some purely altruistic reasons. Fulfilling these actions shows that there is something or someone they care about more than their own person.

As Durkheim explains in his book about suicide, *"A deepest sympathy for human suffering follows the fanatical devotion of primitive times. Each type of suicide is a form of exaggerated or diverted virtue, the manner in which it affects the moral conscience. This does not distinguish suicides enough to have the right to classify them into separate genera."*[28]

As a conclusion to this chapter, altruism is the opposite of egoism. In this case,, the individual is extremely attached to the society and therefore has no life of their own. Altruism

[26] http://sociologyindex.com/egoistic_suicide.htm - Accesed at 11.09.2014.
[27] Emile, DURKHEIM, *Despre Sinucidere*, Editura Institutului European, Iaşi, 2007, p.218.
[28] *Idem*, p.245.

is the main pillar of Hinduist and Buddhist traditions. Self-sacrifice of Buddhist monks during the Vietnam War is the best exemplification of their religious belief system.

4.3 Anomic Suicide

"Society is not just an object that attracts, with unequal intensity, feelings and the activity of the individual, but also a power that can adjust them"[29], explains Durkheim. The term *anomic* is defined as a state of society, characterized by lack of laws or conflicting rules that make it difficult for the individual to orientate in the community. Compared to human individuals, to large or small social groups as a whole, chaos appears as a generator of imbalances.

These inequities are caused by deviations from rules that are recognized and accepted by most people in that society and that is why it has been assimilated with the word *"anomic"*.

Social anomie can be analyzed in terms of motivations and occurrence of deviant behavior within delinquent subculture, being the reaction of protest against the rules of society. From this point of view, there is a social transplantation theory, in which the disruption is considered in corelation with the demoralization of the individual and the occurance of a cvasianomic condition, when talking about the contact between cultures and civilizations. In the process of globalization, the typical anomic criminal activities and methods disperse, move to optimize benefits. They face the supply with the demand of goods, efforts or services like lawful activity, thus generating the occurrence of adverse events for the organization.

Terrorism is therefore one of the anomic manifestations in this violent society, a key concept at the heart of all approaches that aim a certain type of aggressive behavior. This aggressive behavior means committing brutal acts by individuals or groups. Anomic phenomena with global expansion characterized or not by violence, also included computer science and probably could not gain such an extension without the involvement of IT technologies. Using the whole arsenal of tools and software, criminal networks commit frauds, tax crimes and human trafficking by recruiting them from their virtual social sources, organize and carry out illegal migration of a large number of people and falsify documents and money and contribute to money laundering.

The state of anomie occurs when there is a big gap between the individual's goals and the legitimate methods, reachable to certain social categories. In society there are and always will be constant conflicts between the possibilities recognized by law, on one hand the possibility of achieving material and spiritual goals and on the other hand, the real possibilities. Because of these conflicts, the possibilities in reach can be very limited and those social categories of individuals that are not favored resort to illegal means and crime for meeting the goals they set.

The explanation is found in Durkheim's statement which mentions: *"A human being can be happy and mostly live, when his or hers needs are appropriate to the existing possibilities. If they require more than they can have, or something else than they have, then they will always be unfulfilled and they will suffer. A pain that occurs through suffering tends to end at some point. Trends that cannot be met will atrophy and, as the desire to live is a consequence of all those other trends, they can only weaken them together."*[30]

Conclusions

One may think that the term of "suicide" is acknowledged and understood by all. In fact, many common words and concepts that they convey, as *suicide*, can confuse through

[29] http://ssr1.uchicago.edu/PRELIMS/Theory/durkheim.html - Accessed at 01.10.2014.
[30] Emile, DURKHEIM, 2007, *op. cit.,* p.253.

their definitions. Terms and words of this level can be explained only by comparison, as Durkheim mentions, *"A scientific investigation can be complete only if it's based on comparable facts and thus has more chances of success(...)"*[31]

A careful analysis of suicide attacks recorded worldwide highlights their geographical expantion, but not least a diversification of targets targeted by terrorists. By September 11, 2001, suicide bombings had occurred only in certain regions of the world (Middle East and Sri Lanka). This phenomenon later knew a rapid intensification, which led to a sudden concern of those responsible for security. As soon as the terrorist group Al-Qaeda appear, suicide bombings transformed into local and global phenomena.

Suicide has been present since ancient times, and in religious terms, all traditions disagree with the ethics and morality of those who commit suicide. The suicide is the ultimate sin in Catholicism and in most cases is disapproved by Islam, Hinduism, Buddhism, etc.[32]

The initiators of fundamentalism consider that the limits imposed by secular societies aren't yet accepted, and the idea of religion is part of the individual sphere and not of the public one. The most important feature is that fundamentalism wishes *to relocate religion as the center of social life*[33]. Fundamentalism is a global cultural phenomenon. Its aim referes to some social groups that need to resist to rapid changes in society, considering themselves an oppressed groups. Fundamentalism is characterized by the search for ultimate truth and the return to a glorious era "*by restoring the religious society, paradoxaly with the help of modern resources like mass media, bureaucratic institutions and even weapons of mass destruction"* [34].

With psychoanalysis influences, the ideea that suicide would have excessive love features, is perhaps absurd, but as a suicide bomber, love doesn't exist for oneself, but for those whom he will revenge and for its group that choose him to perform this action. The essence of at least one of the psychoanalytic thinking direction, describes suicide as a criminal act directed not against own self, but against *some images of others that have been internalized in itself*.[35]

Aesop's fables *"The Old Man and Death"*, highlights the fact that no matter how hard life is, the happiness to live each day, goes beyond death: An old labourer, bent double with age and toil, was gathering sticks in a forest. At last he grew so tired and hopeless that he threw down the bundle of sticks, and cried out:

"«I cannot bear this life any longer. Ah, I wish Death would only come and take me!»

As he spoke, Death, a grisly skeleton, appeared and said to him:

«What wouldst thou, Mortal? I heard thee call me.»

«Please, sir» replied the woodcutter, «would you kindly help me to lift this faggot of sticks on to my shoulder? »"[36]

Aesop's fable testifies that life has been offered to us to be lived. Self-preservation is written in the our DNA, so that means suicide is a violation of the unwritten rules of life.

Acknowledgement:

This work was possible with the financial support of the Sectoral Operational Programme for Human Resources Development 2007-2013, co-financed by the European

[31] Emile, DURKHEIM, 2007, *op. cit.,* p.9.

[32] Maggie, HELEN, *Despre sinucidere*, Editura Antet XX Press, Bucureşti, 2007 (Original title: Coping with Suicide).

[33] Cristian, BARNA, *Jihad în Europa*. Editura Top Form, Bucureşti, 2008, pp.18-20.

[34] *Idem*, Apud., T., BASSAM, (1998) *The challenge of Fundamentalism: Political Islam and the New World Disorder,* University of California Press, Berkley.

[35] Joiner, Thomas, *Mituri despre sinucidere*, Bucureşti, Ed. Trei, 2013, p. 53.

[36] http://dickens.stanford.edu/tale/print_issue10_allus.html – Accesed at 01.10.2014.

Social Fund, under the project number POSDRU/159/1.5/S/138822 with the title ***"Transnational network of integrated management of intelligent doctoral and postdoctoral research in the fields of Military Science, Security and Intelligence, Public order and National Security – Continuous formation programme for elite researchers - "SmartSPODAS"."***

BIBLIOGRAPHY:

1. ANDREESCU, Anghel, *Organizaţii teroriste. Conceptualizarea terorii vs securitatea europeană*, Editura ARTPRINT, Bucureşti, 2007.
2. ANDREESCU, Anghel, *Organizaţiile teroriste*, Editura ARTPRINT, Bucureşti, 2007.
3. ANDREESCU, Anghel, *Terorismul internaţional - Flagel al Lumii Contemporane*, Editura M.A.I., Bucureşti, 2003.
4. MAIOR, George Cristian, *Incertitudine. Gândire Strategică şi Relaţii Internaţionale în secolul XXI*, Editura RAO International Publishing Company, Bucureşti, 2009.
5. *Studii şi cercetări asupra fenomenului terrorist*, Editura Risoprint, Cluj-Napoca, 2008.
6. TOPOR, Sorin, *O Scurtă Istorie a Terorismului – Comentată şi Interpretată*, Editura Universităţii Naţionale de Apărare "Carol I", Bucureşti, 2013.
7. AUST, Stefan, *Complexul Baader Meinhof*, Editura RAO, Bucureşti, 2011.
8. Duncan, CARTWRIGHT, *Minţi Criminale: Psihanaliza Violenţei şi Crimei*, Editura Trei, Bucureşti, 2010.
9. FRATTASIO, Antonio, *Epistemologia Terorii*, Editura ERA, Bucureşti 2006.
10. RIAZ, Hassan, *Suicide Bombings*, Routlage Publishing, New York, 2011.
11. Kenneth C., RUGE; Barry, LENSON, *Sindromul Othello*, Editura Curtea Veche, Bucureşti, 2012.
12. MURAKAMI, Haruki, *Underground – Atentatul de la Tokyo şi Spiritul Japonez*, Editura Polirom, Bucureşti, 2008.
13. JOINER, Thomas, *Mituri despre sinucidere*, Editura Trei, Bucureşti, 2013.

INFLUENCES ON SECURITY POLICY. BETWEEN STRUCTURE AND AGENT

Mihai ZODIAN
PhD, Junior researcher in the Centre for Defence and Security Strategic Studies within "Carol I" National Defence University, Bucharest, Romania.
E-mail address: zodian@gmail.com

Abstract: *The purpose of this paper is to bring into attention the main factors explaining national security policies, particularly in the area of resource allocation and generation military capabilities. The topic is of importance both because of recent developments in international relations and for theoretical reasons, representing an underestimated research direction after the Cold War. The influences consist of the international power structure, political and social characteristics of actors, and mentalities.*

Keywords: *structuralism, power, culture, elites, social*

Introduction

This paper aims at an explanation of the resource allocation decisions on Defence and endowment policies. The topic is of particular importance in taking into account the public interests, and conceptual reasons, touching upon subjects such as strategic studies, international relations, political science, public policy and military sciences. It was underestimated in the literature from the recent years, while the existing explanations are vague, imprecise and often divergent.

For a long time, explain the dominant theory was that the balance of power in the neorealist version, but it has been criticized both conceptually and empirically. The premises consist of explaining the similarities by structural causes with the balance of power as the main trend of the international system[1]. Since various tests have disproved it, it is clear that the structuralist interpretation should be modified, at least[2].

The many proposals are aimed either at rethinking the relationship between agents and society, or renouncing at power as cause in favour of ideas, political regimes and economic interdependence. Each of them is inspired by realism`s rival research programs, such as constructivism and liberalism. But if from inside the realist program can not be developed a satisfactory interpretation, then it should be at least subordinated to a broader explanation or abandoned.

This approach starts from the core of the theory, as reflected in the works of Hans Morgenthau and Robert Gilpin, and questions the consequences derived from neorealism[3]. The main argument is that the issue of agent-structure should be modified[4], that this can be done inside realism, and that there is a need for a different conception of causality, a

[1] Kenneth WALTZ, *Teoria politicii internaţionale*, Polirom, Iaşi, 2006.
[2] Daniel S. GELLER, J David SINGER, *Nations at war*, Cambridge University Press, 1998; Paul Schroeder, *The Transformation of European Politics*, Oxford, 1994.
[3] Hans Morgenthau, *Politica între naţiuni*, Polirom, Iaşi, 2007; Robert Gilpin, "The richness of the tradition of political realism", *International Organization*, march 1984, pp. 287-304.
[4] Alexander WENDT, "The Agent-Structure Problem in International Relations Theory", *International Organization*, summer 1987.

contextual one, not inspired by statistics. Similar to the neoclassical version, we believe that we can start from Morgenthau, but it is inconsistent press also the structuralist assumption about recurrence balance of power.

1. Restating the issue of structure

Neorealism has established a model composed of principle, functional differentiation and distribution of capabilities[5]. Neoclassical Realism maintained this view, expanding the domestic politics explanation, but its explanatory attempts are insufficient and induce expectations already refuted, such as the superiority of authoritarian regimes in international relations[6].

A theoretical reconstruction must start from a vision of sociability of international actors. The main effort belongs to Buzan and Little, for whom the type of units and interaction capability are defining the international structure prevalent in an era[7]. Adam Watson opened the ordering principle beyond Kenneth Waltz, opposition, for a spectrum comprising independence, hegemony, domination and empire[8].

The structuration theory that influenced these efforts was initiated by Anthony Giddens, explains how systems and capabilities depend on representations of actors for fundamental results, reproducing or radical changing it[9]. This general idea should not turn into an idealist holism style Alexander Wendt, however[10]. We believe it is possible to adapt the essence of argumentation, the dialectic of stability and transformation within realistic tradition, where a series of arguments are compatible.

From a realist perspective, the structuralist conception must start from interests and capabilities, but this not necessarily eliminates the role of ideas and change. For example, one of Morgenthau's principles stated that interests and power are flexible concepts whose meanings depend on ideas[11]. In other words, we can start from the political structure, but the meanings, characteristics and behaviors are influenced by social interpretations, the political culture of an international system.

Interpreting Giddens's theory of structuration close to realism, William Sewell argued that a structure is composed of a schematic element, cultural, virtual, which became manifest depending on the behaviours of the units that use power to reproduce and sometimes change the systemic logic[12]. Their policies are the result of holding some resources and of the ideas about how they can be used[13]. In any social context, we find a variety of structures that interact and produce results which are difficult to predict, including in the same social domain.[14]

---

[5] Kenneth WALTZ, *op. cit.,* Polirom, Iaşi, 2006, pp. 130-143.

[6] Randall L. SCHWELLER, "Bandwagoning for Profit: Bringing the Revisionist State Back In", *International* Security, vara 1994, pp. 74-75; Schweller, *Deadly Imbalances: Tripolarity and Hitler`s Strategy of World Conquest*, Columbia University Press, 1998; Christopher Layne, *Pacea iluziilor, Marea strategie americană din 1940 până în present*, Polirom, Iaşi, 2011. A debate devoted to the actuality of neoclassical realism held was within the Group of Advanced Studies in International Relations, see Octavia Moise (ed.), "Realismul neoclasic la începutul secolului XXI", http://gsari.wordpress.com/2014/10/22/realismul-neoclasic-la-inceputul-secolului-xxi/, accessed on Octobert 2014.

[7] Barry BUZAN, *Sistemele internaţionale în istoria lumii*, Polirom, Iaşi, 2009.

[8] Adam WATSON, *The Evolution of International Society*, Routledge, 1992, pp. 13-14.

[9] Anthony GIDDENS, *A Contemporary Critique of Historical Materialism*, University of California Press, 1981.

[10] Alexander WENDT, *Teoria socială a politicii internaţionale,* Polirom, Iaşi, 2011.

[11] Hans MORGENTHAU, *Politica între naţiuni*, Polirom, Iaşi, 2007, pp. 50-51.

[12] William SEWELL, *Logics of History*, The University of Chicago Press, 2005, p. 136.

[13] *Ibidem*.

[14] *Ibidem*, p. 131.

Thus, in international relations, we can identify political structures, the states system, for example, or economic, such as global capitalism, along with a global culture still being defined, in contrast to local ideational processes[15]. The end of the Cold War can be seen as an interaction between bipolar logic, which required the superpowers to maintain some parity with the politico-military, with the economic one, changing with communicational and informational revolution, alongside with a bigger emphasis of to human rights. In this context. Mikhail Gorbachev tried an accelerated modernization of the Soviet Union, but he failed. The attacks of September 11, 2011 are related to unipolarity and Islamist ideology etc.

Secondly, the international political structure must be specified: following on Gilpin's, Buzan and Little, footsteps, we argue that the predominant type of actor is fundamental for understanding the systemic logic, abandoning the distinction between differentiation as separation and differentiation as role[16]. Dynastic states do not act the same as the national ones; a world based on organizations like the European Union will be different, since the defining principle will be distinct. The political culture can explain how the deep structures are embedded into actor's representations of interest and desirable behaviors, and distribution of power will help us to understand what outcomes are more likely in these circumstances. Following Henry Kissinger, Raymond Aron or Randall Schweller, one can distinguish, based on the presence of shared values, between homogeneous and heterogeneous international political cultures[17].

Thirdly, we must explain how change can occur. Here, the Annales school, anthropology and elaborations of William Sewell can be of much help. The structure can be viewed synchronically, as an international system, or on long term, as a slow process of changes which imprints logics of actions to units, which can react with conformity or they can try to alter. Paul Schroeder, Henry Kissinger and others have shown how the great powers, following the Napoleonic Wars, had built an international order intentionally designed to overcome the limitations of balance of power politics and anarchy, resulting in a partially institutionalized environment, dependent not only capabilities but also a sense of legitimate political action, and Hans Morgenthau explained how it has declined as a result of social and ideological changes[18].

The central determinants are power and events. In neorealism, the power played a conservative function; actors lacking the option to change the system, while for Sewell, units can transfer a domain model to another and mobilize resources to achieve their objectives[19]. Events are times when the structures can be transformed and their conservative or radical nature depends on how the society is defined. They are unpredictable, triggering a chain reaction, at times when the reproduction of the structure through the expansion of its rules to the new situation fails, resulting in a new structure[20]. For example, a change of the idea of sovereignty, accepted by major international actors, defined according to the resources held, will result in a change of the system, even in the absence of a global government.

Starting from on the multiplicity of systems, the political structure defined as a principle, type of units, political culture and distribution of capabilities and from possibilities of transformation defined as normative reproduction failures, one can identify several

---

[15] Barry BUZAN, *Popoarele, statele şi teama*, Cartier, Chişinău, 2000.
[16] Robert GILPIN*, War and Change in World Politics*, Cambridge University Press, 1984.
[17] Raymond ARON, *Paix et guerre entre les nations*, Calmann- Lévy 1962; Gabriel Almond, Sydney Verba, *Cultura civică*, DU Style, 1996; Ruth Benedict, *Patterns of Culture*, Mariner Books, 2006.
[18] Paul SCHROEDER, *The Transformation of European Politics*, Oxford, 1994; Henry Kissinger, *Diplomaţia*, All, Bucureşti, 2007; Morgenthau, *op. cit.* pp. 243-249.
[19] Sewell, *op. cit.*, pp. 131, 143.
[20] *Ibidem*, pp. 227-244.

versions[21]. Thus, an anarchic international system, the dynastic states, balance of power, multipolarity in the eighteenth century; another anarchic, with dynastic states, legitimism, and multipolar in the nineteenth century; one anarchic with pluralism of states, ideological rivalry, multipolarity in the 30s, and another anarchic, characterized by ideological rivalry and bipolarity during the Cold War. Eliminating an ambiguity in the neorealist theory, one must distinguish between conflicts (number of wars and costs) and durability as meanings of stability. A transformation occurs when there is a major disjunction between political culture and distribution of capabilities, compressing this way the explanations provided by Gilpin, Schweller and Sewell.

Through a typological analysis, one can identify some interesting conclusions. For example, multipolar and homogeneous systems seem to be more durable than bipolar, while unipolarity`s future is unclear. The consequences of September 11, 2001, the operations in Iraq and developments in Ukraine indicates a trend of greater heterogeneity, but the results will depend on how the major players will redefine the meanings of the international system, while a new distribution capabilities are sketched our eyes . The idea of a hegemonic cycle valid for four hundred years is questioned because; except the United States after 1989, none of the potential candidates received a special acknowledgment different from the one given to the other great powers.

3.1 The actors and the international system[22]

Structures were defined as contextual constructions and in accordance with structuration theory, as being subject to a double logic of reproduction and change. Actors play an important role, because according to the representations and their resources, one can determine whether or not the international system will be sustainable or conflictual. Neoclassical realism has made an important contribution in their study, but its uncritical acceptance of balance of power theory lead to exaggerated conclusions, as mentioned above, and to allegations of intellectual simplicity.

A realist theory of units must include a vision of states, regimes, the ruling class and capabilities, as factors directly related to the concepts of interest and power. However, the above elements are inadequate, risking a tale quale adoption of authoritarian and elitist vision of domestic policy, which can not explain why the most powerful state in the international system is a democracy. The domestic political culture is necessary because, as shown by Hans Morgenthau, it helps us to understand how interests are conceived, alongside the internal stability and may influence the ability to mobilize resources, as a way of strengthening the legitimacy of the authority.[23]

Actor's general capability is a first fundamental factor. They identify the international position, but also the potential that institutions can use to generate power, including the Defence policies[24]. However, they do not automatically translate into military force since the transformation depends on other factors, like the representations of elites. Consequently, although power constitutes a fundamental element, a reductionistic approach is too simplistic. Thus, one we can say that the overall level of Defence capabilities influences resource allocation and procurement, but not by a rigid determinism.

---

[21] Kalevi HOLSTI, *Peace and war, Armed Conflicts and International Order 1648-1989*, Cambridge University Press, 1991.

[22] I wish to express my gratitude towards Radu Ungureanu for clarification of some ideas.

[23] Robert COX, "Social Forces, States and World Orders", în Robert O. Keohane, *Neorealism and its critics*, Columbia University Press, 1986, pp. 218-219.

[24] Andrei MIROIU, *Balanţă şi hegemonie*, Tritonic, Bucureşti, 2005.

The discussion regarding the state was relaunched by Barry Buzan with the distinction between strong and weak entities, based mainly on legitimacy of the authorities[25]. A rival criterion refers to the autonomy they hold in relation to civil society[26]. The second was considered ambiguous, but it can not be abandoned and we suggest reformulation in the tradition of Samuel Huntington, as existence of a functional division of political institutions[27]. The extraction capacity varies depending on the existence of a complex organizational system, which contributes to a more efficient allocation of taxation, although it may induce conflicts and negotiations for distribution.

The type of political regime helps us to understand what values are promoted through public policy and how they are distributed[28]. Totalitarian and authoritarian regimes are theoretically more concerned with the development of the armed forces, but too high a concentration may affect long-term latent power. Consequently, democracies are characterized by periodic controversy regarding the allocation of resources, but on the long term they tend to allocate resources to Defence. Authoritarian regimes can allocate large resources in the short term, while risking exhaustion[29].

Elites are found in the majority of modern societies, and from the perspective of security policies it matters the nature and type of representation/ideas which prevails. One should consider, first, their degree of pluralism, while the dualistic typology of Schweller's requires nuances[30]. A unified elite can allocate major resources for the security sector, but is vulnerable if society was modernizes. More groups tend to press the political system, competing for redistribution of rights and wealth[31]. The divided ones look more flexible, but they are unable to build a consensus. Pluralist and consensual elites will engage in complex negotiations to allocate resources among different policies, but they are more stable in the long run[32].

Culture includes representations elites and legitimacy of governance institutions[33]. The first issue concerns the degree of internalization of rules system, contrary to Wendt, which is oriented towards conservation logic; we prefer to keep open the possibility of change. Consequently, regardless of the source and intensity of motivations, interests balance theory taking, we can classify the status quo and revisionist actors[34]. The second, shown by Robert Jervis, is about a model refers to the predominance of offensive versus defensive handling security issues[35]. The third refers to the degree of contestation and justifications offered by ruling groups to get the necessary support follow different policies. Here, one may note the

---

[25] Barry BUZAN, *Popoarele, statele şi teama*, Cartier, Chişinău, 2000, pp. 104-115.

[26] Andrew BENNET, Joseph Lepgold, Danny Unger, "Burden-sharing in the Persan Gulf War", *International Organization*, vara 1994; Robert D. Putnam, "Diplomacy and Domestic Politics: The Logic of Two-Level Games", *International Organization*, vara 1988.

[27] Samuel P. HUNTINGTON, *Ordinea politică a societăţilor în schimbare*, Polirom, Iaşi, 1999.

[28] Raymond ARON, *Democraţie şi totalitarism*, All, 2001, pp. 21-24.

[29] Bruce Bueno de MESQUITA, Alastair Smith, *Manualul dictatorului*, Polirom, Iaşi, 2012, pp. 253-277.

[30] Randall SCHWELLER, *Unanswered Threats*, Princeton Universitz Press, 2008; Randall L. Schweller, „Unanswered Threats: A Neoclassical Theory of Underbalancing", International security, Fall 2004, pp. 180-181.

[31] Ralf DAHRENDORF, *Conflictul social modern*, Humanitas, 1996.

[32] Robert DAHL, *Poliarhiile*, Institutul European, 2000. Arend Lijphart, *Modele ale democraţiei*, Polirom, Iaşi, 2006.

[33] Roland H. EBEL, Raymond C. TARAS, James D. COCHRANE, *Political culture and Foreign Policy in Latin America*, Suny Press, 1991. See also Stanislav Secrieru, *Rusia după imperiu*, Institutul European, 2008, pp. 29-46 şi Emanuel Copilaş, *Geneza leninismului romantic*, Institutul European, Iaşi, 2011.

[34] Randall L. SCHWELLER, "Bandwagoning for Profit: Bringing the Revisionist State Back In", *International* Security, vara 1994, pp. 74-75 şi *Deadly Imbalances: Tripolarity and Hitler`s Strategy of World Conquest*, Columbia University Press, 1998.

[35] Robert JERVIS, *Perceptions and Misperceptions in International Politics*, Princeton University Press, 1976.

level of acceptance and the inclusiveness of actor's forms of legitimating, but the second aspect is correlated with government representation. An offensive political culture tends to increase the resource allocations for Defence; a similar effect is produced by the existence of accepted authority. Internalization, alongside capabilities, is linking the system with the units.

Of these variables, select social coalitions and power relations within the elite and the political culture, where we find both strategic and institutional explaining Defence procurement policies. One can see here same juxtaposition of power and structure as in the discussion of the international system, as evidenced by Sewell, with influences from historical sociology, especially Esping-Andersen, Barrington Moore but also historians like Fernand Braudel, Pierre Renouvin or Paul Schroeder[36]. The overall aim of the approach is the refining of realism. They summarize many variables and causal mechanisms, like regimes, stratification and traditions, taking into account that reality can not be captured fully.

All things being equal, an extended social coalition tends to allocate resources in a diversified manner between various groups. Therefore, the trend will be a reduction or moderation of investment for security, at least in the short term. In the medium and long term, it may lead to the functional development of public institutions and increase overall welfare, including the Defence capabilities.

A revolutionary political culture, with an offensive model of international relations and benefiting from ample support will encourage the development of the armed forces. The defensive revolutionary and the status quo and defensive system of values will promote programs for mid-level procurements. The status quo, defensive and peaceful ones should be restricted to prudent weapons programs.

Conclusions

We started with the idea that a neorealist explanation for building capabilities is inadequate in order to elaborate a revised version. The international political structure was conceptualized in terms of capabilities, but also cultural, to encompass both aspects covered by theorists. Internally, the main explanatory variables of adopting different policies endowment were social coalitions prevailing and the political culture.

Acknowledgement:

This work was possible with the financial support of the Sectoral Operational Programme for Human Resources Development 2007-2013, co-financed by the European Social Fund, under the project number POSDRU/159/1.5/S/138822 with the title ***"Transnational network of integrated management of intelligent doctoral and postdoctoral research in the fields of Military Science, Security and Intelligence, Public order and National Security – Continuous formation programme for elite researchers - "SmartSPODAS"."***

BIBLIOGRAPHY:

1. ALMOND, Gabriel, VERBA, Sydney, *Cultura civică*, DU Style, 1996.
2. ARON, Raymond*, Democraţie şi totalitarism*, All, 2001,

[36] Barrington MOORE jr., The Social Origins of Dictatorship and Democracy: Lord and Peasant in the Making of the Modern World, Penguin Books, f. l., 1966, 1974; Gøsta Esping-Andersen, *The Three World of Welfare Capitalism*, Princeston University Press, 1990; Fernand Braudel, *Mediterana şi lumea mediteraneană în timpul lui Filip al II-lea,* Meridiane, Bucureşti, 1985-1986; Pierre Renouvin, *Histoire des Relations Internationales*, Hachette, 1994, vol I-IV.

3. ARON, Raymond*, Paix et guerre entre les nations*, Calmann- Lévy 1962.
4. COPILAŞ, Emanuel, *Geneza leninismului romantic*, Institutul European, Iaşi, 2011.
5. MOORE jr., Barrington *The Social Origins of Dictatorship and Democracy: Lord and Peasant in the Making of the Modern World*, Penguin Books, f. l., 1966, 1974.
6. BENEDICT, Ruth, *Patterns of Culture*, Mariner Books, 2006.
7. Bennet, Andrew, LEPGOLD, Joseph, UNGER, Danny, "Burden-sharing in the Persan Gulf War", *International Organization*, vara 1994.
8. BRAUDEL, Fernand, *Mediterana şi lumea mediteraneană în timpul lui Filip al II-lea,* Meridiane, Bucureşti, 1985-1986
9. DE MESQUITA, Bruce Bueno, SMITH, Alastair, *Manualul dictatorului*, Polirom, Iași, 2012.
10. BUZAN, Barry, *Popoarele, statele şi teama*, Cartier, Chişinău, 2000.
11. BUZAN, Barry*,Sistemele internaţionale în istoria lumii*, Polirom, Iași, 2009.
12. COX, Robert, "Social Forces, States and World Orders", în Robert O. Keohane, *Neorealism and its critics*, Columbia University Press, 1986, pp. 218-219.
13. DAHL, Robert, *Poliarhiile*, Institutul European, 2000.
14. DAHRENDORF, Ralf, *Conflictul social modern*, Humanitas, 1996.
15. ESPING-ANDERSEN, Gøsta, *The Three World of Welfare Capitalism*, Princeston University Press, 1990.
16. GELLER, Daniel S., SINGER, J. David, *Nations at war*, Cambridge University Press, 1998.
17. GILPIN, Robert, "The richness of the tradition of political realism", *International Organization*, March 1984.
18. GILPIN, Robert*, War and Change in World Politics*, Cambridge University Press, 1984.
19. GIDDENS, Anthony, *A Contemporary Critique of Historical Materialism*, University of California Press, 1981.
20. HOLSTI, Kalevi, *Peace and war, Armed Conflicts and International Order 1648-1989*, Cambridge University Press, 1991.
21. HUNTINGTON, Samuel P., *Ordinea politică a societăţilor în schimbare*, Polirom, Iași, 1999.
22. JERVIS, Robert, *Perceptions and Misperceptions in International Politics*, Princeston University Press, 1976.
23. LAYNE, Christopher, *Pacea iluziilor, Marea strategie americană din 1940 până în present*, Polirom, Iași, 2011.
24. LIJPHART, Arend, *Modele ale democraţiei*, Polirom, Iaşi, 2006.
25. MIROIU, Andrei, *Balanţă şi hegemonie*, Tritonic, Bucureşti, 2005.
26. MORGENTHAU, Hans J., *Politica între naţiuni*, Polirom, Iași, 2007.
27. MOISE, Octavia (coord.), "Realismul neoclasic la începutul secolului XXI",
28. http://gsari.wordpress.com/2014/10/22/realismul-neoclasic-la-inceputul-secolului-xxi/ (accesat octombrie 2014).
29. PUTNAM, Robert D.,"Diplomacy and Domestic Politics: The Logic of Two-Level Games", *International Organization*, vara 1988.
30. RENOUVIN, Pierre, *Histoire des Relations Internationales*, Hachette, 1994, vol I-IV.
31. SCHROEDER, Paul, *The Transformation of European Politics*, Oxford, 1994.
32. SCHWELLER, Randall L., "Bandwagoning for Profit: Bringing the Revisionist State Back In", *International* Security, vara 1994.
33. SCHWELLER, Randall L., „Unanswered Threats: A Neoclassical Theory of Underbalancing", International security, Fall 2004

34. SCHWELLER, Randall L., *Deadly Imbalances: Tripolarity and Hitler`s Strategy of World Conquest*, Columbia University Press, 1998.
35. SECRIERU, Stanislav, *Rusia după imperiu*, Institutul European, 2008.
36. SEWELL, William, *Logics of History*, The University of Chicago Press, 2005.
37. WALTZ, Kenneth N., *Teoria politicii internaţionale*, Polirom, Iaşi, 2006.
38. WATSON, Adam, *The Evolution of International Society*, Routledge, 1992.
39. WENDT, Alexander, "The Agent-Structure Problem in International Relations Theory", *International Organization*, summer 1987.
40. WENDT, Alexander, *Teoria socială a politicii internaţionale,* Polirom, Iaşi, 2011.

ANALYSIS OF RESISTANCE TO CHANGE AS A SPECIFIC RISK OF MILITARY ORGANIZATION

Dumitru Cătălin BURSUC
Commander (Navy) Engineer, PhD candidate in Military Science and Information,
"Carol I" National Defence University, Bucharest, Romania.
E-mail address: catalin258@yahoo.com

Abstract: *The risks in the military organization cannot be analyzed separately from the modern armed conflicts. Nowadays, more than 20 million people have left their home because of armed conflicts, their exodus carrying not only the population problems, but inducing potential dramatic consequences, directly or mediated, in this regard we note that over 40% of the refugees around the world are children. Military actions or the humanitarian ones are no longer offering solutions in satisfactory ways for these problems. It is required an integrated model of analysis and planning of activities at any level, so the prevention becomes an essential component of activity at all levels.*

The organization must respond with structural changes and adaptation of the specific tasks to new realities and how these influence their missions and military structures. Also, the specific normative basis which provides the integrated management risk in the Ministry of National Defence requires be evaluating and reconsidering.

Keywords*: risk management, military organization, effective action.*

1. Risk assessment in the Organization

The present and the development of the phenomena and processes at the global level are characterized by a permanent state of change. The assessment of the risks to which organizations are exposed must take into account this dynamic and to translate it into specific instruments which ensure an optimal management planning functionality. Actions which in the past were harshly blamed and had a reduced practicing area, are getting extended now, thus in 75% of the current conflicts children are used as combatants or in suicide bombings.[1]

Social practice and the elementary logic confirm that the risks cannot be identified and evaluated in their entirety. At the opposite pole lie the practice of risks denial and the type of attitude that an unknown danger doesn't affect you.

The managerial practice shifts from dealing with the risks and assuming them to a stage of systematic analysis and measurement of risks and designing of their management measures.

The current normative framework allows the management to overcome the reactivity and the imposition of a proactive behavior in managerial exercise. For this purpose, at the organizational level, risk management is included in the internal control management framework, providing such systematic tools for diagnosing, monitoring or managing the risks associated with organizational activity.

[1] UNHCR, *2008 Global Refugee Trends: Statistic Overview of Population or Refugees*, Internaly Displaced Persons and other Persons of Concern to UNHCR, in http://www.unhcr.org, accessed at 20.05.2014.

The Institute of Internal Auditors establishes a point of evolution in how risks are addressed at the level of the Organization[2], regardless of the nature of the organization.

Risk management becomes an integral part of the internal audit, the process being characterized by the following:

- the internal audit has a major role in risk evaluation in organizations;
- the risk management activity is likely to bring real value to the Organization;
- the internal audit has the obligation to create the system of risk assessment, where it does not exist.

The risk is regarded as any factor that may have an impact on the capacity of the Organization to achieve its objectives. In this situation, the nefarious action has to include the auditor due to errors or lack of good faith. Thus, risk management provides a methodology, providing a comprehensive risk management which enables the Organization to achieve the best cost in terms of controlled exposure to risk.

Risk factors are appreciated to be any deficiencies, nonconformities, irregularities of the environment or organization which, in the context of the occurrence of certain events, will cause unfavorable effects to the entity in question.[3] International practice in the field recognizes as consecrated risk factors the following:

- lack of cohesion of the team management and misunderstanding or ignorance of the employees for the strategy;
- unclear delineation of responsibilities within the Organization, lack of fluency and flexibility of the information circuit;
- violating or ignoring the rules;
- interrupting of the flows of activity due to the departure of a person, loss of documents, activities in the area of disasters, strikes, etc..
- the lack of trust in its activities with third parties, which will affect decisions;
- the lack of competitiveness of human resource, products or services;
- the lack of job control, managerial incompetence stations and lack of trust in the managers;
- image problems of the organization, conflict of interest, fraud etc..

Conceptual integration of the elements listed in the description converges to the organizational pathologies characterized by lack of flexibility and adaptation at the level of the Organization, reactive attitude and permanent post-factum response to changes in the environment.

The regulatory framework must be doubled in structures and the responsible actors in the organization, which must plan and implement from the decision-making positions, concrete measures to streamline.[4]

All these elements are found in the current practice of military organization, however, due to the specificity of the military organization the elements acquire particular ways of manifestation.

2. Resistance to change in the military organization as a risk factor

As an open system, the military organization has directly, only the internal control and only with limited adjustment possibilities of the efficiency, the reference targeting the military

[2] In 2002 the Institute of Internal Auditors has fundamentally altered the internal audit process and how risks are treated in this process.

[3] V. Ionescu, Analiza modului de operare a managementului riscurilor în instituţiile sectorului public din ţările membre ale U.E. – referat de cercetare ştiinţifică nr. 1, Universitatea Naţională de Apărare „Carol I" , Bucharest, 2010, p. 27.

[4] David Brooks, Security risk management: A psychometric map of expert knowledge structure, in Risk Management, Volume 13, Issue 1-2, 2011, Publisher Palgrave Macmillan, Basingstoke - United Kingdom, p. 17.

action where the influence of the activity is staff attribute.[5] Other people outside the organization, through their actions, are introducing elements of influence on external environment. This absence of control and adjustment through direct feedback, at the macro social level is decided by internal mechanisms such as:

- the military conduct required, much firmer than in any other social domain;
- the obligations, the deprivations and the system of punishments and rewards .

The possibility of reduced external control causes a higher stiffness in the military institution and, in the same time, gives the military organization a greater stability over time, but generates institutional inertia towards the adaptation to social changes in comparison with the rest of society.

The strict normative regulation characterizes military organization, the need of norms in the military domain being one of the highest because:

- military system, as such, is highly complex, the stake of the shares in the system being victory (success) in a violent relationship with an enemy, it should be noted that a number of consequences of the action, as well as the error or failure, they have, unlike other systems of human action, an absolute existential-value condition.[6] The effects of the assumed risk are huge material damages and, most dramatically, the loss of human lives.
- unlike all the other systems of organization and human action, the military system is featured by triple poses of action status: the status of peace, the status of war and the intermediary status between these two ends of the spectrum of conflict.[7] This triple posture determine both the high need for normalization (otherwise being unable to effectively change the system state by preserving its existence and by guaranteeing the ultimate goal achievement, the system is threatened by the risk that, in respect of damage in terms of changing the status of the transition to the status of war), and the extremely strong specialization of military rules.

The transition to the knowledge based economy and less on conventional raw materials and physical work, occurs in close correlation with the economic and social transformations which induce changes in the nature of military action. This framework requires a new understanding of the relationship between war and a society in rapid change[8], including a new understanding of the ways of adapting the military organizations in the process of global social change.

Usual change generates a waiver of stability, at the conditions and context of action entered into the habit; this fact, coupled with the impossibility of controlling the future announced through change, causes uncertainty justified by risk factors and their consequences.

Conclusions of the studies from last two decades highlight the importance of the way of understanding and reporting of humans to the change, identifying factors appreciated as being at risk, which causes resistance to change, as well as:

- lack of information on the objectives and purposes of the change, with results lack of motivation;
- information relating to the acceptance of change is effective when there is homogeneity of the members of the organization, possible only for small organizations.

The act of driving the change is a strategic activity for a commander [9], for a leader of the military organization must identify and be familiar with the characteristics of the military

---

[5] Simion Boncu, *Securitatea europeană în schimbare. Provocări şi soluţii*, Editura Amco Press, Bucureşti, 1995, p. 45.
[6] Mihaela Vlăsceanu, *Psihosociologia organizaţiilor şi conducerii*, Editura Paideea, Bucureşti, 1993, p. 124.
[7] Alexandru Stoica, *Teoria conducerii organizaţiilor militare*, Editura A.I.S.M., Bucureşti, 1998.
[8] Alvin Toffler, *Power shift*, Editura Antet, 1995.
[9] Gheorghe Arădăvoaice, , *Comandantul (şeful) – profil psihoprofesional*, Ed. A.I.S.M., Bucureşti, 1994.

organization, to understand the specifics of each of these in the functioning of the mechanism of military organization to allow intervention in enhancing the effectiveness and efficiency of operations.

Military regulations fix the behavior of members and that, not only formally but also outside it. The behavior is expressed through external symbols, such as: military attire, military ranks, insignias, conduct, etc., and are aimed at identifying the militaries as a distinct group, united through a formal link that generates power, influence and authority. The importance of the formal link is the consequence of the establishment of strict rules imposed by the military laws, orders and regulations. This does not mean that the military organization meet formal relations only. During the performance of the tasks and activities is the manifestation of the informal relations. In all cases, however, the formal relationship prevails.[10]

The concept of bureaucratic institution means:

- exclusive vertical subordination;
- activities on the principle of unity of command;
- increase of the discipline role and the order in carrying out organizational cohesion;
- specialized roles and the status;
- hierarchy of functions and ranks[11].

Looked in this perspective, military organization is not established as a result of individual choices, but on determined objective criteria which take into account the capabilities, skills and military availability to perform tasks.

Military hierarchy is distinguished from other cases in that it establishes the group's social stratification. Social distance between the positions occupied by the officers, non-commissioned officers, and soldiers gives rise to internal organizational phenomena, which must be given the necessary attention, which, sometimes, are likely to block or hold organizational transformation processes. A good understanding and awareness of the effects of social stratification in the military organization requires a comprehensive and interdisciplinary approach, and, as practice, requires dedication and consistency from the leader.

The army is the core component of the armed forces, which is providing in peacetime and at war, integration into a unified conception of the activity of all the forces participating in the actions of national defense. The representative of the fundamental interests of Romania subordinated to the people's choice, the army has the fundamental mission of safeguarding the sovereignty, the independence and unity of the State, the territorial integrity and the constitutional democracy [12].

The military organization acts for the performance of the tasks in the integrated framework with the components of the national system of defense, public order and national security, such the organizational transformation affects and is affected by the interdependence of all elements of this system.

3. The solutions of process nature to the problem under review

Internationally, it manifests the tendency of the crystallization of the theoretical apparatus and instruments for risk management, fact with direct implications for organizational performance.

---

[10] Ion Ciocan, Negreţ, Ion, *Formarea personalităţii umane. Semnificaţii şi sensuri instructiv – educative*, Ed. Militară, Bucureşti, 1981, p.186.
[11] Constantin Onişor, *Teoria strategiei militare*, Ed. A.I.S.M., Bucureşti, 1998.
[12] *** *Legea 45/1994 privind Apărarea Naţională a României.*

The literature[13] groups the trends which are elements to exceed organizational resistance to change, in the following main directions:

- reporting to the stakeholders and certifying that the risks have been identified, but confirms the fact that the need of transformation exists and is functional;
- the evaluation and promotion of benefits arising from the change in the effective management of the organization;
- continuous improvement of institutional strategies and methods of risk management.

The current practice in the field sets organizations that manage risk through identification and analysis and then evaluate whether the activity should be amended by treating risk, in order to meet the criteria for risk[14]. In carrying out the process, the organizations make public the information and shall consult with shareholders, monitor and verify the risk level and the instruments to ensure control, means that the changes of consequences to ensure that it is not necessary for a return to risk treatment. Thus, ISO 31000 is the international standard governing risk management. This standard describes in detail the systematic and logical process can be used by any organization, it is not specific to any domain and any industrial area and can be applied to any type of risk.

For organizations of every type and size is necessary a reaction for a range of risks which are likely to have an impact on the planned targets.

Risk assessment is part of the management that identifies the way in which objectives may be affected and analyzes the risk in terms of their likelihood and consequence of occurrence, prior to the decision, if is necessary a future treatment. In this regard the standard SR EN 31010 / 2010 – *The Risk Management-Risk assessment techniques*, comes in support of ISO 31000 and provides regulations on the selection and implementation of systematic techniques to risk assessment. This standard aims to reflect best practices applied in selection techniques and the implementation of risk assessment techniques and does not refer to new or emerging concepts which have not achieved a satisfactory level of professional consensus [15]. A process way to approach the resistance to a change like risk in military organization is shown in the following figure.

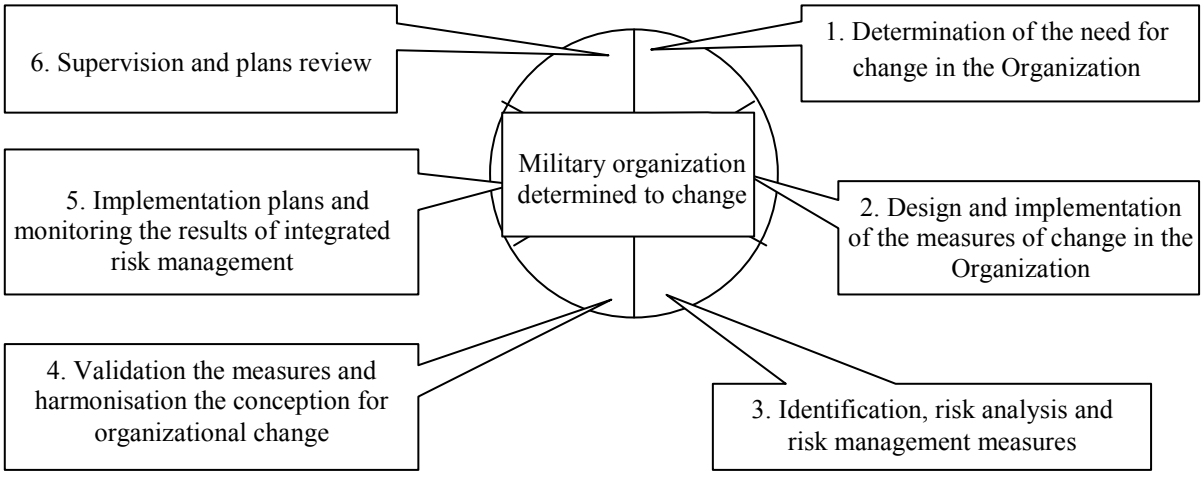


Figure no. 1. The treatment process of the resistance to change like risk in the military organization

[13] Coord. Aurel BURCIU, *Introducere în management*, Editura Economică, Bucureşti, 2008, p. 541.
[14] Standardul ISO 31000 / 2009 *Managementul riscului. Principii şi linii directoare*, în http://www.consultanta certificare.ro/stiri/standardul-pentru-managementul-riscului-iso-31000.html accesat la data de 30.06.2013.
[15] http://www.consultanta-certificare.ro/stiri/iso-31010.html, accessed on 28.06.2014.

In the Ministry of Defense we apply a national framework of *the Methodology of implementation of internal control standards risk management,* in Ministry of Defense *Order no. M-235/2007*[16]. According to these terms, each public entity has an obligation to examine systematically, at least once a year, risks related to the conduct of its activities, to develop appropriate plans in the direction of limiting possible consequences of these risks and to designate responsible for the implementation of these plans.

Final considerations

Within the permanent growth of the influence of environment on organization, risk assessment is necessary to be done with full compliance of phases and procedures, the activities of control and self-control, with permanent adaptation and updating. Only in this way one can ensure efficient activities depending on the evolution of risks.[17]

The current regulatory framework, prior to the recollected one, is insufficient and fails through the content and practical measures integrated with enhanced efficiency risk management in the activities of the military organization.

In the military organization the design of risk management programs is required to provide valuable actions proportional to the level and intensity of risks, you need them to be prioritized and directed from the simple to the most difficult to control. Resistance to change in the organization is not reported as risk for organizations and is not appreciated as the specific situation for the military institution.

A review is required, and later, by planning, it is necessary to develop the consistent measures, with applying the same methods for similar situations, being generalized in this way the positive experience, success in the activity of the organization. The situations of instability regionally or globally, what are the characteristic of generalized economic crisis periods, require more the concrete analysis and appropriate measures to manage the risks in any type of organization. [18]

Acknowledgement:

This work was possible with the financial support of the Sectoral Operational Programme for Human Resources Development 2007-2013, co-financed by the European Social Fund, under the project number POSDRU/159/1.5/S/138822 with the title ***"Transnational network of integrated management of intelligent doctoral and postdoctoral research in the fields of Military Science, Security and Intelligence, Public order and National Security – Continuous formation programme for elite researchers - "SmartSPODAS"."***

BIBLIOGRAPHY:

1. ARĂDĂVOAICE Gheorghe, *Comandantul (şeful) – profil psihoprofesional*, Editura A.I.S.M., Bucureşti, 1994.

[16] Controlling the elements of this standard is the responsibility of the General Secretary in MoD;

[17] In Annex B.2 of standard SR ISO IWA 2 - Quality management systems-guidelines for the application of ISO 9001/2000 specified measurements which accompanied by a grid that is determined by the minimum accepted value, can provide a set of operational tools for the establishment of performance indicators in identifying.

[18] This work was possible with the financial support of the Sectoral Operational Programme for Human Resources Development 2007-2013, co-financed by the European Social Fund, under the projectnumber POSDRU/159/1.5/S/138822 with the title "Transnational network of integrated management of intelligent doctoral and postdoctoral research in the fields of Military Science, Security and Intelligence, Public order and National Security – Continuous formation programme for elite researchers - "SmartSPODAS".

2. BONCU Simion, *Securitatea europeană în schimbare. Provocări şi soluţii*, Editura Amco Press, Bucureşti, 1995.
3. BROOKS J. David, *Security risk management: A psychometric map of expert knowledge structure*, in Risk Management, Volume 13, Issue 1-2, 2011, Publisher Palgrave MacMillan, Basingstoke - United Kingdom, pp. 17-41.
4. BURCIU Aurel (Coord.), *Introducere în management*, Editura Economică, Bucureşti, 2008.
5. CIOCAN Ion, NEGREŢ Ion, *Formarea personalităţii umane. Semnificaţii şi sensuri instructiv – educative*, Editura Militară, Bucureşti, 1981.
6. IONESCU V., Analiza modului de operare a managementului riscurilor în instituţiile sectorului public din ţările membre ale U.E. – referat de cercetare ştiinţifică nr. 1, Universitatea Naţională de Apărare „Carol I" , Bucureşti, 2010.
7. ONIŞOR Constantin, *Teoria strategiei militare*, Editura A.I.S.M., Bucureşti, 1998.
8. STOICA Alexandru, *Teoria conducerii organizaţiilor militare*, Editura A.I.S.M., Bucureşti, 1998.
9. TOFFLER Alvin, *Power shift*, Editura Antet, 1995.
10. UNHCR, *2008 Global Refugee Trends: Statistic Overview of Population or Refugees*, Internaly Displaced Persons and other Persons of Concern to UNHCR, în http://www.unhcr.org.
11. VLĂSCEANU Mihaela, *Psihosociologia organizaţiilor şi conducerii*, Editura Paideea, Bucureşti, 1993, p. 124.
12. *** *Legea 45/1994 privind Apărarea Naţională a României, actualizata;*
13. Standardul ISO 31000 / 2009 *Managementul riscului. Principii şi linii directoare*, în http://www.consultantacertificare.ro/stiri/standardul-pentru-managementul-riscului-iso-31000.html.
14. http://www.consultanta-certificare.ro/stiri/iso-31010.html.

THE NECESSITY FOR CHANGE OF ATTITUDE TOWARDS RISK IN THE MILITARY ORGANIZATION

Dumitru Cătălin BURSUC
Commander (Navy) Engineer, PhD candidate in Military Science and Information,
"Carol I" National Defence University , Bucharest, Romania.
E-mail address: catalin258@yahoo.com

Abstract: *Risk management process provides the basic structure for identifying, assessing and controlling risk. Commanders at all levels must identify and plan the response to risks in an integrated process. Carrying out the mission of a military structure requires knowledge and multiple risk-taking activities with high bias for the decision maker in the organization.*

Defining the risk of an undesirable event that can decrease the effectiveness of the action or compromise it, we automatically associate it to the uncertainty of achieving the planned outcome. Uncertainty refers to the probability of occurrence of an event, the effect of the event or processing possibilities, courage, determination and ability to assume the associated consequences of an event, that the leader has. It is obvious that the attitude towards risk in the organization is related to the ability to identify risk factors and assess their importance, to the way consequences are anticipated and their influence on the planned objectives.

Keywords: *risk management, risk attitude, attitude types.*

1. Assessments on attitude towards risk in the military organization

Risk management has as fundamental objective to increase of operational capabilities and improve the conditions for the execution of missions, while keeping losses of any kind to a minimum acceptable level. Risk management, in general, adopt principles, standards and operating procedures applicable to all levels for conduct of activities in the organization[1] and fundamentally contribute to the conservation of resouces and maximizing efficiency and effectiveness.

Military organization's actions involve, by their nature, exposure to risk. For this, organization develops levers and mechanisms supporting the monitoring and control of risks. Along with displays of formal and institutional expression we encounter, we mention less standardized or informal situations from risk management practice. Manager's attitude towards risk is included in these less standardized situations.

The specific activity of the organization, but also a simple reasoning, confirms that risks cannot be identified and evaluated in their entirety, but the wording does not exclude the manifestation of this type of attitude. Right the opposite appears the practice of denying the risk, attitude saying that an unknown danger does not affect you.

For a risk assessed as major, the commander asks the assigned staff to perform risk reduction, reflected by the inclusion of additional safeguards measures in the estimation model.

[1] B. RITCHIE, C. BRINDLEY, *An emergent framework for supply chain risk management and performance measurement* , in The Journal of the Operational Research Society, suppl. Risk Based Methods for Supply Chain Planning and Management**,** 2007, p. 1399.

Depending on the results of the re-estimation to the safeguards measures included, a new plan may then include a new request for reduction or risk sharing.

Ideally, one expects that estimators or risk assessors and managers to be different, circumstances specifically required for quantitative risk estimation. In reality, the military organization in our country does not have specialized personnel designated with distinctive attributes by the organizational charts.

The work that treats military organization distinguishes between manager, ruler and leader. In this approach, the manager is the member of the organization appointed or elected in a formal institutionalized manner in a management position with responsibilities. The ruler is any person in a leadership position (can be a manager, but also the person holding the leading position of non-economic organizations, like political parties, public institutions, worship, an organizational subsystem as groups, work teams or compartments or informal group), different from the first case is the person who set up this structure. About the leader, we say that it's the person (formal or not) with the greatest influence on members in an organization, influence recognized and accepted by all staff or by the vast majority of them, based on emotional relationships. The three roles are not mutually exclusive, so the manager can be a leader, and usually rulers have powers and duties of management.[2]

2. Necessary skills for risk management in military organization

Based on the previous paragraph, it is obvious that the maximum advantageous position is when the informal leader overlaps or is found in the person of the leader or manager of the organization. In this respect, it follows logically that the management-leadership relationship is a whole-part relationship, in which the desired matrix for the position of manager is made from the leader's characteristics. By extrapolation, we appreciate that not every genuine leader is a good manager of military organization, but a successful manager is necessarily a leader of the same level. Without expanding the theoretical discussion, we mention here that leadership concerns that process of social influence in which one person guides, coordinates and motivates the group to achieve the objectives in organizational context[3].

Regarding military organization leadership from this complex perspective, the risk management process requires people with complementary skills: to be able to identify and treat risks, to motivate staff so that action to enable the management of available resources in order to transform inputs into good results, thus realizing generation of capabilities.

Achieving goals, but particularly carrying out tasks, require the leader to have specific professional skills: interpersonal, knowledge, technical, persuasion[4]. A more complete description is provided by the works on the military domain[5], thus, the commander's skills are: relational, communicational, conceptual, technical, analytical, decisional, IT&C. An operational structuring distinguishes skills grouped by: technical skills, such as accounting or marketing, cognitive skills, analytical mind and conceptual ability and traits related to emotional intelligence, such as self-knowledge and relational skills[6].

---

[2] Filaret SÂNTION, Aurel PAPARI (coordonatori) – *Psihologie organizaţională*, Editura Fundaţiei Andrei Şaguna, Constanţa, 1999, p.213.

[3] Septimiu CHELCEA, Petru ILUŢ – (coordonatori) – *Enciclopedie de psihosociologie*, Editura Economică, 2003, p.157.

[4] James GIBSON, John IVANCEVICH, James DONNELLY – *Organizations*, Irwin; McGraw Hill, Boston, 1997, p. 275.

[5] Constantin ROMANOSCHI, *Basics Management, Defense Resources Management,* Note de curs, Departamentul Regional pentru Managementul Resurselor de Apărare, Braşov, 2001, p. 59.

[6] Daniel GOLEMAN, Richard BOYATZSIS, Annie Mckee - *Inteligenţa Emoţională în leadership*, Editura Cartea Veche, Bucureşti, 2005, p. 333.

The classification includes rational and emotional dimensions of psychological characteristics with volitional-actional dimension, these helping to strengthen the role of attitude in the risk management process.

Leaders are those who have full capacity to influence the emotions of all[7]. The complex describes emotional intelligence containing 4 domains and 18 competencies:

1. self-knowledge: emotional self-awareness, correct self-evaluation, self-confidence;
2. self-control: emotional self-control, transparency, adaptability, ambition, initiative, optimism;
3. social awareness: empathy, organizational conscience, solicitude;
4. managing relationships: inspired leadership, influence, training others, catalyze change, conflict management, team spirit and collaboration.

These skills underpin leadership styles that are multipliers of group effort. The characteristics of emotional intelligence are not innate factors, but learned skills and each one is in compliance in particular ways to leader's ability to mobilize personnel, understanding resonance with the effect of leader effectiveness.

3. The balance between the aspiration of winning and fear of failure

The decision and its implementation has as motivation a result of two reasons mediated by the structures of the commander's personality: gain aspiration and motivation to avoid failure. The activity in risk situation cumulates both reasons. Attitude towards risk is dependent on the composition of the relative strength of the desire for success and fear of failure, meaning the ratio of the motivation to achieve / avoid failure (Mf) and the motif of searching the success (Ms).

The common goal of a class of motives is to maximize satisfaction by providing necessities or needs. The achievement reason is considered an approach to success[8].

The goals achieved by comparing the two indices results in the classification of subjects in:

- subjects oriented towards success (Ms> Mf);
- subjects oriented towards editing to failure;
- subjects in which Ms = Mf.

Stimulus value (I) is defined in terms of probability of success / failure. We consider that, for a tough to accomplish task (with a low probability of success), the satisfaction of success is high and disappointment is small. The incentive value of success (Is) is positive: Is = 1-Ps and incentive value of failure (If) is negative: If = (-Ps), where Ps is the probability of success.

Decision makers motivated by fear of failure will issue, when at risk, extreme decisions. Easy tasks (with high probability of success) are attractive because the threat of failure is minimal. Preference for those chances has a substantial psychological significance. Picking a heavy task (situation) protects the image on himself of the subject even in case of a failure "whoever lost in a situation so difficult". Internal risk is reduced and increases a sense of security by taking external risks.

Due to the subjective probabilities' change (their increase after success and decrease after failure), the subject with MS < Mf will behave paradoxically[9]. After a success, they will be inclined to take fewer risks, if initially chose a risky option, or remain at an easier task, while after failure they will want to choose a more difficult task than that caused failure or loss.

---

[7] Daniel GOLEMAN, Richard BOYATZSIS, Annie MCKEE, *Op. Cit*. p. 23.
[8] Mihai GOLU, *Dinamica personalităţii*, Editura Geneze, Bucureşti, 1993, p148.
[9] http://consultantaeducationala.ro/lucrare-de-licenta.php, accesat la 05.09.2014.

4. Types of attitudes towards risk

The main attribute of risk management is that it continuously seeks to capture the complex relationships between specific objectives of a structure, vulnerabilities associated to processes that support the achievement of these objectives and threats to effective achievement of objectives.

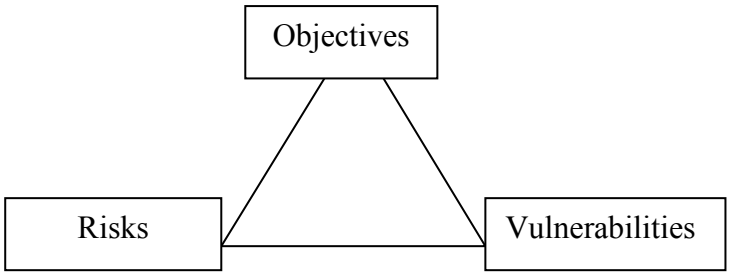


Figure no. 1. The relationship objectives - risk - vulnerability

Vulnerabilities require timely and efficient management, otherwise they are liable to turn into threats and therefore in risks.

When taking a risk, a person is attracted by the prospect of gain and removed from that of loss, which he seeks to minimize. It is known, however, that the risk and its consequences are not always repulsive for the decider. There are situations in which the individual rejects the decision with lower risk alternatives, being attracted by the higher risk. In his decisions, he tends not so much to the minimum level of risk, but to a risk level appropriate to its physical structure.

We recognize two categories of factors[10] that contribute to the definition of risk-taking tendency:

- contextual factors generated by reference to case;
- structural factors resulting from the tendency to excessive risk taking and inappropriate instrumental behavior.

How the manager relates to risk situation, the meaning he attaches to assuming or avoiding risk-taking have close relationships with his personality. Depending on the specific of fundamental nervous processes, several differences are highlighted at the objective level of risk finding, at the subjective level of treating the risk and the degree of realism with which the individual evaluates his behavior at risk. All this shows that the freedom in the manager's decision making supports a number of restrictions of personal, subjective nature, if there are some key factors involved in developing decision under risk.

The temperament is a psychological dimension of the person and is recognized as a defining variable in determining individual behavior under risk.

There are approaches that have attempted to establish correlations between individual decisions and the personality structure of each individual. There are classifications that describe the following human types that manifest specifically in the decision process under risk[11]:

- the receiver is tempted to get everything from outside, does not act on its own initiative, expects decision variations, he does not take a decision by himself;

[10] Alexandra HOROBEŢ, *Managementul riscului în investiţii internaţionale*, Editura All Beck, Bucureşti, 2005, p.64.
[11] Mihaela VLĂSCEANU, Psihologia organizaţională şi a conducerii, Bucureşti Editura Paideia, 1993.

- the operator does not produce ideas, but take from others by force and guile, he uses others;
- the keeper accumulates, saves, fears of waste, refrain from making decisions involving a risk factor;
- the merchant lacks firm principles, is fluctuating, takes relatively fast decisions without thinking too much about consequences, opt for choices that bring advantages;
- the producer, ideal decision-maker with the balance of size gain / risk dimension.

The literature suggests two decision types[12] described by manifest characteristics.

Type A behavior is considered as a collection of behaviors triggered in some people in specific environmental conditions. It is characterized as an actional - emotional complex translated by aggressive involvement in a chronic struggle to achieve a grouping of activities in a time as short as possible, regardless of the obstacles. This type is described by the following psychological symptoms and personality characteristics: competitiveness, sharp ambition, critical and self-critical spirit, persistent desire for recognition, involvement in multiple and diverse activities, accelerated implementation, hostility and aggression in interpersonal relations, dominated by the feeling "rush" and "urgency", the tendency to evaluate psychosocial factors as creating the feeling of insecurity status, motivation for achievement and success, dominance, anxiety, stress and depression, irritability and impulsivity, low disconnection and relaxation capacity.

Subjects defined as belonging to type B presents the opposing attitudes of the subjects of type A.

Summarizing the behavior described in terms of involvement in the decision making under risk, decision makers share in:

• success-oriented;

• oriented to avoid failure.

The cognitive approach, the act of deliberation and the response to some risk situation is a result of the numerous features of the person dealing with the unpredictable and objective conditions.

5. Possibilities to adequate the attitude towards risk

The unpredictable situation with regard on the consequences of the outcome probabilistic dependence on the adopted variant and external influences, makes assessment of effectiveness to be very complex in the case of decision making under risk. Post factum is easy to appreciate how good it was to be operated, it is important to determine ante-factum the most appropriate action.

We review some optimal situations of decision under risk:

a) the manager takes into consideration for the activity the determination of the biggest disadvantage that may arise and then selects the least disadvantageous strategy, one whose case is the least damaging predicament;

b) in military action the analysis is oriented towards the worst situation for its own structure and the strategy of the opponent causing it. This is where the strategy of the enemy under any other strategies may be more disadvantageous than that was analyzed.

c) optimistic attitude implies that whatever you choose, it will produce the most favorable consequences. The commander conducts chosing the strategy that has among the

[12] Gabriela Florenţa POPESCU, Ioana OMER, *Dimensiuni compensatorii ale stresului la nivel organizaţional*, în Cercetări filosofico-psihologice, Academia Română - Institutul de Filosofie şi Psihologie „Constantin Rădulescu-Motru”, ianuarie–iunie 2011, BUCUREŞTI, pp. 99-100;

most favorable possible consequences, whatever the risks arising from the choice of this action alternative.

d) we recall one of the analytical methods, the Hurwicz method, that sets as chosen variant the weighted average of the minimum and maximum gains. This action variant is based on the usefulness, bearing the name of optimism criterion.

e) by the maximization of expected value the principle of insufficient substantiation is utilised. The manager will choose the option with the highest expected value, because it is believed that one has no information on the relative probabilities of consequences, so it accepts all as being equal to each other.

Military action requires success now and here and not failures that dissipate their losses in a total amount of actions. In modern conflict, due to precision dynamism and strokes force, the fight engages knowing that, whatever the outcome, a second battle may not exist. In the presented cases, certain criteria of rationality can lead to another recommendation in a risk situation and what is rational according to some, to be unthinkable for another. Choosing a variant of action must be based on the situation, objectives and missions and take into account the significance of risk taking for the manager.

6. Discussion on intuition and creativity as an alternative sollution

Current practice shows that managers use their intuition power to make decisions. Studies show that intuition has been often used, especially as a mechanism for evaluating the rational decisions.

A fair question raised in the literature[13], is whether managers can be taught to use their intuition. After testing more than 10,000 managers, it concluded that in most cases, high management positions are filled by people with high degree of intuition[14]. Organizations need both analytical and intuitive personalities to operate at full capacity.

Intuition is important and instincts must be followed, especially when managers have a rich experience and special results. Intuitive action must be correlated with unexpected events, with high dynamics and low degree of predictability. Note that intuition is no substitute to reasoning, especially with the existence of new technologies that can analyze large amounts of information in lesser time.

Organizational environment dictates the conditions under which people work, and they can stimulate or inhibit creativity. Inhibitor factors of creativity include: fear of job evaluation, careful monitoring during work and excessive competition in the team or between teams. On the opposite, creativity stimulation is given by the feeling of autonomy, belonging to a team with diverse skills, creative colleagues and supervisors[15]. Cordial and supportive relationships with bosses are attributes of creativity. Flexible organizational structures and participatory decision-making processes are also associated with creativity. Organizational framework, however, can also raise obstacles to creativity[16]. They can be represented by centripetal and centrifugal tendencies within the group, by intense criticism of new ideas, by domestic competition lacking constructiveness and excessive risk avoiding.

Leaders can play important roles in shaping creative behavior. The organizational culture can encourage risk taking and reward innovation. Both intuition and creativity have

[13] O. BEHLING, N.L. ECKEL, *Making sense out of intuition*, Academy of Management Executive, 5, pp. 46-54;
[14] W.H. AGOR, Intuition in organizations: *Leading and managing productively*. Newbury Park, CA: Sage Publications, 1990, p. 263.
[15] J. ZHOU, *When Presence of Creative Co-workers Is Related to Creativity: Role of Supervisor Close Monitoring, Developmental Feedback, and Creative Personality*, Journal of Applied Psychology, 2003 Jun;88(3):413-22.
[16] T. M. AMABILE, S. G. BARSADE, J. S. MUELLER, B. M. STAW, Affect and Creativity at Work, Administrative Science Quarterly, 2005, 50, pp.367-403.

major influences on management decision-making process. These concepts need further cultivation as an alternative to traditional attitudes in response to risk. We appreciate that managers need to better understand how to use techniques to stimulate intuition and creativity to develop employees and to make effective decisions.

Acknowledgement:

This work was possible with the financial support of the Sectoral Operational Programme for Human Resources Development 2007-2013, co-financed by the European Social Fund, under the project number POSDRU/159/1.5/S/138822 with the title ***"Transnational network of integrated management of intelligent doctoral and postdoctoral research in the fields of Military Science, Security and Intelligence, Public order and National Security – Continuous formation programme for elite researchers - "SmartSPODAS"."***

BIBLIOGRAPHY:

1. AGOR W.H., Intuition in organizations: *Leading and managing productively*. Newbury Park, CA: Sage Publications, 1990.
2. AMABILE T. M., BARSADE, S. G. MUELLER J. S., STAW B. M., Affect and Creativity at Work, Administrative Science Quarterly, 2005, 50, pp.367-403.
3. BEHLING O., ECKEL N.L., *Making sense out of intuition*, Academy of Management Executive, 5, pp. 46-54.
4. GIBSON James, IVANCEVICH John, DONNELLY James – *Organizations*, Irwin; McGraw Hill, Boston, 1997.
5. GOLEMAN Daniel, BOYATZSIS Richard, Mckee Annie - *Inteligenţa Emoţională în leadership*, Editura Cartea Veche, Bucureşti, 2005.
6. GOLU Mihai, *Dinamica personalităţii*, Editura Geneze, Bucureşti, 1993.
7. HOROBEŢ Alexandra, *Managementul riscului în investiţii internaţionale*, Editura All Beck, Bucureşti, 2005.
8. POPESCU Gabriela Florenţa, OMER Ioana, *Dimensiuni compensatorii ale stresului la nivel organizaţional*, în Cercetări filosofico-psihologice, Academia Română - Institutul de Filosofie şi Psihologie „Constantin Rădulescu-Motru", ianuarie–iunie 2011, BUCUREŞTI, pp. 99-100.
9. RITCHIE B., BRINDLEY C., *An emergent framework for supply chain risk management and performance measurement* , in The Journal of the Operational Research Society, suppl. Risk Based Methods for Supply Chain Planning and Management, Nov 2007, pp. 1398-1411.
10. ROMANOSCHI Constantin, *Basics Management, Defense Resources Management,* Note de curs, Departamentul Regional pentru Managementul Resurselor de Apărare, Braşov, 2001.
11. SÂNTION Filaret, PAPARI Aurel (coordonatori) – *Psihologie organizaţională*, Editura Fundaţiei Andrei Şaguna, Constanţa, 1999, p.213.
12. VLĂSCEANU Mihaela, *Psihologia organizaţională şi a conducerii*, Bucureşti Editura Paideia, 1993.
13. ZHOU J., *When Presence of Creative Co-workers Is Related to Creativity: Role of Supervisor Close Monitoring, Developmental Feedback, and Creative Personality*, Journal of Applied Psychology, 2003 Jun;88(3):413-22.
14. http://consultantaeducationala.ro/lucrare-de-licenta.php, accesat la 05.09.2014.

ORGANIZATIONAL CULTURE AND MILITARY INSTITUTION – CONVERGENCES AND DIVERGENCES

Dan GOGOESCU
ROU Land Forces Staff / military personnel, PhD candidate in Management,
Faculty of Economy and Business Administration, Craiova University.

Abstract: *The deficiencies, cleavages and negative aspects regarding the build up, existence and continuity of organizational culture within the public institutions are far more important – as effect and implications – when take place the particularization / specialization of that public institution. When this "specialization" concerns the field of assuring the national security (national defence), the aspects regarding the development of an adequate organizational culture from all points of views is essential. Of course, such institution – from the defence field – imply already the existence of some own norms and rules for functioning, but this not means that we can not state that can exist also another type of organizational culture, specific. In reality, it is supposed, directly and without doubt, that precisely the institutions from defence field have their own organizational culture, each term from the concept's definition (applied to these institutions) find its image in the existence of the institution itself, this having clear, distinctive features from those connected with civilian public life, the regulations and the Guide of the military activity and career being materialized in palpable proves of these institution's organizational culture. And, still, the reform of military institution, on all its levels, requested and imposed by the new security environment, internal and external, regional and global, will have to take into consideration also the crystallization of a new type of organizational culture, harmonized with values of so-called traditional military culture.*

Keywords: *organizational culture, military institution, reform of military affair, management, management of human resources, guide of individual career.*

Introduction

There are some theories about the relations between the concepts of *national culture* and *culture of organizations from public field*, the concept of *culture of organizations* appearing due to the complex process of globalization, due to the fact that each community has its own system of common values, similar experiences or perceptions regarding the external environment, accepted and shared by each member of this community. The multitude of these perceptions and expressions related with the multitude of specific communities in a certain space (territorial) cumbered the process of creation a specific pattern of the organizational culture in institutions, public or private. The „difficulties" which appeared during the process were reflected in the difficulty to determine the dimensions of the concept of culture, referred to the concept of the organizational culture in private and public organizations.

It could appear an elementary process and resemblance if we bring together the organizational culture in a public defence institution and the military institution culture. Still, there are a lot of analogies among them, living simultaneously with a lot of differences. It can be appreciated that the military institution is the best reflection of what an organizational culture means, but the organizational culture in a public institution can not be compared with the organizational culture of a military institution due its distinctiveness. In the globalization

era, the structure, elements, principles and characteristics of the concept of organizational culture is "borrowed" by different countries and communities, despite the location, which could and suppose to enrich those societies/communities on all level and aspects. Furthermore, the globalization process added complexity to what can be defined as concept of organizational culture but, in the case of the Romanian society, this complexity was accompanied by the insecurity, the value's scale depreciation, disorientation and confusion when we are talking about honour, respect, sense of duty related to the *national culture,* referred to the country itself. A careful analysis of what is positive and what can harm an organizational culture within the military could put on the right track the future evolution of that institution and the future development of the specific organizational culture.

1. The organizational culture and the public institutions

The dimensions analysed by different specialist in the specialized literature take into consideration the extremely wide dimensions of the researches (Kluckhohnand Strodbeck approach-5 dimensions, Fons Trompenaars -7 dimensions and Geert Hofstede - 5 dimensions, during 2010 added the sixth) regarding the common issues of the societies, without taking into consideration the space and time (location and time period).

The Kluckhohn and Strodbeck[1] studies showed that the common issues of all societies are connected with the particularities of character of human nature, his relation cu nature, the temporal settlement, the *modus vivendi* of individuals and the types of the relations among them. The people can not primarily good or bad, but only a mix of this. Normally, the dynamic adaptability to the external environment is a characteristic of the individuals, being essential for their surviving. These authors take into consideration 3 possible types of human relations: individualist, collateral and lineal, the collateral type could be assimilated with the collectivist type, and the lineal type emphasizes the relations among different generations.

Fons Trompenaars transferred his studies on international level, identifying the practical aspects of the international affairs in terms of seven cultural dimensions (universality versus particularity, individualism versus collectivism, emotional cultures and neutral cultures, specific cultures versus diffusive cultures, status and relations with nature).

Geert Hofstede[2] had the most complex approach, allowing the comparison between state's cultures. He established a relation between *national culture* and *organizational culture* starting from other dimensions than his predecessors (*distance from power, individualism − collectivism, masculinity – feminist, avoiding the incertitude, orientation on long term/short term*). So, *the distance from power* is unequal, the size depending by the hierarchical structures, the dimension being very visible in family, school and at job. In a certain organization, a large distance from power means that managers and subordinates are on different hierarchical levels and a short distance from power means subordinates equal to managers. In Hofstede`s vision, the dimension *individualism − collectivism* represents the *level in which a society values the personal objectives, autonomy, intimacy, commitment toward the group's rules, implication in collective activities, social cohesion and intense socialization*[3]. Hofstede defined the individualist societies as societies where the relations among its members are chaotic, egocentric, while the collectivist societies are composed by people who are integrated from birth in strong subgroups, where they are protected during their lives; the only service requested in exchange being total loyalty. So, in an individualist

[1] Kluckhohn, F.R.& Strodbeck, F.L. *Variations in Value Orientations*, Row, Peterson & Co, 1961.
[2] Hofstede, G. *Culture's Consequences: International Differences in Work Related Value*, Sage Publications Inc, Beverly Hills, 1984.
[3] Hofstede, Geert, Gert Jan Hofstede & Michael Minkov. *Cultures and Organizations: Software of the Mind,* 3rd Ed. New York: McGraw-Hill. 2010.

culture the individuals-employees will act according to their own interest, which will be organized in order to coincide with their employer's interest, while in a collectivist culture the employees will act as part of a subgroup of common interests. Currently, in Romania, this dimension is distorted, the negative aspects being the so-called "nepotism" or "professional heirs". In numerous situations, the positive aspects are changing in negative aspect, the "honour" of a certain family being realized ignoring, despising the other members of society, the individualist attitude and the creation of an overbearing position, totalitarian, quite egocentric being main actions of such individuals. The dimension of "avoiding the uncertainty" represents the measure in which the members of a certain culture feel threatened by unknown situations. Within the societies where there is no uncertainty, there are many un/official rules which control the rights and obligations of employer and employee. Again, the sociological studiers realized in Romanian society showed that this dimension is orientated negatively, the retained rules being those concerning the assuring the continuity of bribes, nepotism, power, supremacy of money and instauration of vulgarity and ill-breeding manners. The last dimension identified by Hofstede shows the measures in which the values are oriented toward future, the opposition to past or present (respect for traditions, fulfilment of social obligations). Unfortunately, the last one are values characteristic to the cultures from countries with orientation on long term, respectively to Asian countries and less to Romania where, during the last years, there to few positive examples in this respect[4].

Each from the above mentioned studies and specialists have its own limitations, deficiencies and contributions, but still they became background of culture's analysis and, subsequently, generated what was called *organizational culture in the public institutions*.

In a society with a strong culture she will have a huge influence over the institutions and their performances, the concept of organizational culture being defined similarly to the concept of national culture[5]. Linda Smircich stated that "culture is a set of values, dense beliefs, conceptions and habits of mind, all shared by the members of an organization, to whom it will be presented as being accurate"[6], while the Romanian specialists[7] appreciate that *organizational culture in the public organizations can be understand as the sum of distinctive, spiritual, material, intellectual and affective features outcome from the individuals habit of mind, sentience and personality, displayed in work processes which determine significantly the mission of public organizations and their fundamental objectives.* The components of organizational culture are similar with those of national culture, to these been added a new concept – organization's mission. The organizational culture is supposed to offer the organisation's members a sentiment of an organizational identity, of common values, needs and ideals[8]. Normally, the ideas of organizational culture derive from the core of organization, from its first leaders who articulated and implemented ideas and values as a vision, philosophy or strategy. If these ideas and values lead to performances, they are institutionalized giving birth to a certain organizational culture.

2. Organizational culture and the institutions from defence branch

The deficiencies registered during evolution of the organizational culture within the public institutions are extremely important, as effects and implications, in the case of the

[4] Daniel GOGOESCU, *Particularities of the organizational culture in the public institutions from the defence field – between neccessities, requests and possibilities - in course of publishing in* Academy of Economic Science Paper - Management Challenges for Sustainable Development. Bucharest. Romania. 2014.
[5] L. COPELAND, & L. GRIGGS, *Going International*. New York. Plum Books. 1987.
[6] L. SMIRCICH, *Concepts of Culture and Organizational Analysis*. Administrative Science Quarterly. 1989, p.28.
[7] A. ANDRONICEANU, *Management public*. Editura Economică. Bucharest. 1999.
[8] E. SCHEIN, *Organizational Culture*. American Psychologist 45. 1994.

institutions from national security field. Of course, such institutions imply own regulations, a specific code, but that does not necessarily coincide with a specific organizational culture. In fact, in reality, it is presumed directly and without doubt that mainly the institution from the defence field have their own organizational culture, the definition of the concept, applied to these institutions, comprehending the *sum of distinctive, spiritual, material, intellectual and affective features resulted from the individuals habit of mind, sentience and personality, displayed in the work processes and which significantly determine the mission of the organization from the defence field and its fundamental objectives*[9]. Each term of this definition is reflected in the specific code of the military institution, which already has distinctive features from those from civil ones, the rules and guide of the military activity and career being relevant proofs of the organizational culture of this type of institution.

The components of the organizational culture within the military institution follows, generally, the patterns of national culture to which is added the "organization's mission", these bestowing the specific identity and affiliation to the organization through common values, needs and ideals. The ideas of this organizational culture comes from the organization's background, retained from founders till present, which are not bend or subject to changes and which were materialized in state defence, the national sovereignty and Romanian people. Still, unfortunately, this specific organizational culture abided some distortions, dysfunctions and alterations[10], the only positive part being given by the fact that these irregularities didn't, yet, touch the core of the military institution, which could be fatal for the state itself.

The elements which can have effect upon organizational culture in civil institution can be also applied in the case of organizational culture of military institution, but their impact is diminished by specificity of this institution. The strong cultural values promoted by the military institution's leaders are shared by each member of organization from training till employment in organization, the effort to convey the message to the employees being smaller than in the case of civil institution due to its steadiness characteristics (on long and very long term). The codes of military conduct already assign a "road" for every individual who follow a military career, with precise norms and going through pre-established stages.

In the Romanian military institution is easier to determine the representation's forms of the noticeable aspects of organizational culture, materialized in *storiettes, symbols, heroes, rites, ceremonies and rituals, language, norms* and *status*. We are used to hear, from generation to generation, such "storiettes", perceived some times as fairy tales, more or less pleasant. By contrast, the civil institutions, where the high rhythm of changes is generated by the turmoil of political sphere, the *storiettes* led to the birth of "nightmares", where hated heroes are politicians or their representatives, chosen or appointed in leading public positions. These *storiettes*, *symbols*, *heroes, rites, ceremonies, language, norms* and *status* within the military institution are easier and faster noticed, analysed, catalogue, building up – easier and faster - the crystallization process of organizational culture specific to military institution.

Unfortunately, the persistent degradation of international security environment, of the organizational culture from public (civil) and, partially, private institutions, generated the distortion of certain elements of military institution's organizational culture such persistence, perseverance, parsimony and even honour, the relation network through status and function.

---

[9] Daniel GOGOESCU, *Particularities of the organizational culture in the public institutions from the defence field – between neccessities, requests and possibilities - in course of publishing in* Academy of Economic Science Paper, Management Challenges for Sustainable Development, Bucharest. Romania. 2014.

[10] These are going from "swoons" in employment process for different categories of personnel, wrong structure of the job`s pyramid, lack of certain specialists and lack of personnel implication in career`s development till disinterest, detachment of the personnel (Oniciuc Corduban, Ionel. *The management of the individual career in Romanian Army in the new regional and global security environment.* National Defence University "Carol I". Bucharest. 2011).

The admission of our country in structures with regional or global character do not brought only benefits to the military institution's members. Giving up the conscription, induced difficulties in promoting the military career, recruitment and selection of professional human resources, and also the insufficient career management[11] had a direct and indirect impact over the fulfilment of military organization's mission, sometimes not acceptable.

Maintaining the state defence capability to expected high standards, reducing the man power, changing the force structures, these are activities which suppose to increase the role of the management (at all levels and types) in order to assure the necessary professional human resources for the institution. The military institution wants and have to be "modern, flexible, adequate shaped and equipped army, deployable, capable to attend to a large range of missions on national territory or abroad, according to the diversity and complexity of its missions, (…) including to those concerning the multinational operations of crisis management and fighting against terrorism"[12]. In order to achieve these objectives it is necessary to reform, conceptual and structural, the military institution, its management, its conception and leadership.

The time showed us that not any desire to follow a military career can be materialized, no matter whether is due to individual's characteristic or his abilities The transition of the Romanian economy toward the market economy generated a strong negative effect of erosion of traditional values (patriotism) and the immediate consequence for the military institution was the dissolution of the military career`s allure, materialized in diminish number of military personnel. To this can be added the decrease of birth rate, more tempting offers on civilian job market, bearing on military institution's performances[13].

The analysis of the civil (and military) personnel`s situation in the Romanian military institution (from the professional structure, usability and evolution's possibilities in career points of views), registered not substantial changes from previous years, in certain aspects the situation goes worse and a reform it is more than requested[14]. On the execution level, the difficulties appeared also because of the mix of civilian–military personnel and there are situations when the civilian posts were set up on general pattern, without a precise hierarchy of these posts, without possibility to rise from the ranks. In the case of leadership position (regarding the political appointments)[15] the situation is no better, mainly to the fact that each leader brings his (own) staff, in many situation ignoring the existent – and sometimes, qualified – civilian personnel. Furthermore, despite the attempt to assimilate the civilian jobs with the military through internal norms, practically it is ignored, the simple remembering of this order generating conflicts at workplace[16].

The organizational culture in the military institution is demure also by the deficiencies of current professional evolution of the civil personnel, the absence of the adequate remuneration based on different level of responsibility and competence, lack of motivation and decrease number of high professional competent personnel civil or military -, existent or

---

[11] Ion, GURGU. *The Professional Human Resources Management of Defence in context of Romanian Armed Forces Reform. Implications over the Romanian Military Art.* National Defence University "Carol I". Bucharest. 2007; Oniciuc Corduban, Ionel. *The management of the individual career in Romanian Army in the new regional and global security environment.* National Defence University "Carol I". Bucharest. 2011.

[12] Ionel, ONICIUC CORDUBAN. *The management of the individual career in Romanian Army in the new regional and global security environment.* National Defence University "Carol I". Bucharest. 2011. p.6-7.

[13] Ion, GURGU. *The Professional Human Resources Management of Defence in context of Romanian Armed Forces Reform. Implications over the Romanian Military Art.* National Defence University "Carol I". Bucharest. 2007; Oniciuc Corduban, Ionel. *The management of the individual career in Romanian Army in the new regional and global security environment.* National Defence University "Carol I". Bucharest. 2011.

[14] *Idem*.

[15] A. ANDRONICEANU, *Noutăţi în managementul public*, Editura Universitară, 2006.

[16] Daniel GOGOESCU. *Difficulties of the individual career management in defence field - in course of publishing in military publication*. 2014.

supposed to be employed in future. During the last years it was registered a high number of demission of civil and military personnel, with specific competences, due to the lack of adequate professional gratification and a better remuneration. Due to the pre-created reputation of the military institution`s stability, currently, there are selected only civilian personnel who have no aspirations for a superior career (with medium training/performance levels or having a certain age).

An adequate management should joint institution`s and individual`s needs, understand correct and complete the factors of influence which usually "disturb" the individual's choice of a career, his evolution in career, determining the crystallization of a complete and adequate organizational culture. The individuals located in a permanent changing environment - technical and technology, education and training, social and economic situation, occupations mobility or disappearance of certain specialization – need a very careful planning of career, advised by professionals.

The military institution enacted regulatory documents regarding the professional evolution of its employees, „getting over to an individual career management which is unitary and flexible, based on professional competence, performance and development potential, his application, is a difficult and on long period process"[17]. Still, there were registered deficiencies generated by the partial application of the principle of decomposing the execution policies and inexistence of a real organizational and individual planning, which led to a fractional personnel resources management. In these circumstances it is difficult to build up an adequate organizational culture or to maintain, in acceptable coordinates, the previous ones. Other deficiencies consist of those generated by the decrease level of standards regarding the admission in a military institution, the abusive use of the indirect channel to "form" the military personnel in incondite branches from the military organizational structure, the non-unitary settlement of the military specialities for which is called on to the development on indirect channel and to the evolution of the military personnel originated from this channel within the military hierarchy[18].

The invisible aspects of the organizational culture in military institution, affected by the external distortions, concerns the "dilution" of the national solidarity`s sense, the attitude toward the country's defence, the social cohesion, the conformation to communitie`s norms, disrespect and disappearance of the Romanian military traditions and values and the false impression that this institution is not concerned by its personnel situation (current and future).

There is a characteristic of the national and organizational culture on Romanian society level which has a positive impact over the organizational culture in the military institution, and we are talking about the *regional culture* (which begins from the national culture values and is varying in different geographical regions of the country). If, on the civilian public institutions level, this particularity highlight the cleavages among the organizational culture of the public institutions on regions (going from the employees of the Transylvania's public institutions who are looking for performance, attachment to the institution where they are working, respect and responsibility spirit, professional conscience, through Muntenia`s public employees who are more concerned in obtaining a social and professional status, money, high welfare, while the organization's importance is on second

[17] Daniel GOGOESCU, *Difficulties of the individual career management in defence field - in course of publishing in military publication*. 2014.

[18] Daniel GOGOESCU, *Particularities of the organizational culture in the public institutions from the defence field – between necessities, requests and possibilities - in course of publishing in* Academy of Economic Science Paper, Management Challenges for Sustainable Development, Bucharest. Romania. 2014; Gurgu, Ion. *The Professional Human Resources Management of Defence in context of Romanian Armed Forces Reform. Implications over the Romanian Military Art.* National Defence University "Carol I". Bucharest. 2007; Oniciuc Corduban, Ionel. *The management of the individual career in Romanian Army in the new regional and global security environment.* National Defence University "Carol I". Bucharest. 2011.

plan, to Moldova`s public employees who are looking for collaboration with other persons, going to conform to the institution`s traditions and ceremonies, showing hospitality, open organizational spirit, tolerance to other peoples, concerning for maintain their jobs, a.s.o.), in the military institution these aspects of regional organizational culture tend to homogenize, supporting its development in a faster rhythm. Furthermore, these specificities are building up to a certain base – military code – determined by the training/education in certain military educational facilities[19].

Altogether, the human resources management system existent in military institutions tend to progress positively, its main issue remains the "volatile" decisions/actions of keeping the valuable personnel within the system, the elimination of existent lack of "appeal" toward the development of career in military institution, despite the limited/absent financial possibilities. The military instruction's reform must be approached as a system of systems, strongly connected; the process must be implemented on all levels (doctrines, forces organization and structure, capabilities, intelligence activity, training, education, acquisitions, personnel management and budget planning). Naturally, this must also imply changes on the level of organizational culture, the innate wish being that these "changes" will take into consideration only the positive aspects of the concept.

Conclusions

No matter what model is used in analysis, it come out the fact that, for the public employees, the present is more important, they being even "reluctant" to their future or the future of their public institution where they are working. Most of them consider that the future is a matter of their bosses and of the political elites, despite the fact they feel the negative effects in a larger proportion than their leaders. In fact, the leaders consider that it is important what is happening currently, the future being pretty vague and difficult to predict. Also, the best scenarios imply that the public employees have a carelessness attitude.

On the level of inter-human relations from public institutions, these do not fulfil, totally, their role to complete the structure of formal organizational relations and to strengthen cohesion of the informal groups, which are established within these institutions, going more toward the development of interest and power networks. Generally, the public employees admit that they prefer to respect the very rigid norms which exist in institutions, without taking into consideration the possible negative implications of this attitude over the final results of their activity and, implicitly, over their clients. Furthermore, there are many cases where they admit that they intercede in order to solve their friend's issues, their personal obligations, when they wish to develop relations with those persons, even if the existent general norms are affected.

They also mentioned the fact that there is a tendency to increase the individualism within the public institutions. Beside the increased level on non-implication and avoiding to take initiatives within the public institution, it started to institute – on alarming level – the attitude to non-assume responsibilities (individual or on group). Their justification is that the initiative is not encouraged neither stimulated, in many cases being punished. In this respect, the negative behavioural manifestation earns a higher weight in creating a distorted organizational culture within those public institutions.

[19] A. ANDRONICEANU, *Noutăţi în managementul public*, Editura Universitară, 2006; Onea, Angelica-Nicoleta. *Diversitate culturală în management: o abordare interregională.* Editura Universităţii "Alexandru Ioan Cuza". Iaşi. 2011; http://www.adrnordest.ro/user/file/leader/manual-leadership-in-dezvoltare-regionala.pdf-Agenţia pentru Dezvoltare Regională Nord-Est. Manual de Bune Practici. Leadership în Dezvoltare Regională. 2012.

The above mentioned behaviour is incompatible with the wish of the public employees to accede to a higher status, they considering that the detained titles are very important. So, the above mentioned dimension *distance toward power*, in this case, is distorted, existing large hierarchical distances, the leadership style being authoritarian one. It is preferred the responsibilities delegation but without allowing the assumption of the positive results (only the negative will be assumed, and they are followed by punishment) and of some possible benefits, reason for which, the public employees wait till they receive an order in which is specified what to do, to receive a written document about a future assignment to be fulfilled, if this assignment differs – in its content – by the tasks which they usually have to fulfil.

All above mentioned facts determine weak connectivity - as intensity – among the individuals of an institution, and they are displayed, mainly, only within small groups, in informal sphere. The distortions which appear in this case bear in mind the establishment of a false organizational culture, generated by the persons employed on the recommendation of persons from interior or exterior or persons who belongs to a common interests subgroup (as variation from the well-known nepotism behaviour).

The reality proved that the values of the organizational culture from public institutions determine, significantly, the productivity of public services and the fulfillement of the provisioned objectives. These, unlike other values categories, must permanent adapt to the economic, social, legislative, political, administrative existent context, in a determined period of time. The incompatibility among the initiated changes in a public institution and the values of organizational culture represents the main reason of pitching and failure of public institution itself. In order to avoid such situations it would be recommended to determine the effects which the values of the public instruction's culture have over the processes which are going on inside that institution, the public employees expectations and even of the political elite involved in the public management in public institutions.

The reality confirms that there no successful unique models of organizational culture, each public institution having its own specificity, despite the existence of certain valuable universal cultural values, written or not. To take into consideration only these elements and eliminate or diminishing the importance of other, is huge mistake. The most obvious example, and the easier one, is that of the public defence institutions. Hereby, the emphasis of the values which are specific to organizational culture, the appliance of culture so that balance the general/common with the particular, the universal with the specific, means not only the success of public manager, but also of the management process from that institution.

The organizational culture and performance are, obviously, connected and the reality proves that, if an organization is changing pretty often its public managers and a part of its employees become open to the risk of weakening its organizational culture, could be on the road to losing its cultural identity, which, on medium term, could affect the general balance of the public institution. Each step of the process to solve the issues generated by the changes from external environment must imply obtaining the consensus for the new values determined by the strategy, purposes, means, measurement of performance, motivation a.s.o. The organizational culture in public institutions – even those in defence field – cannot assure the institution's stability if every change, no matters if it comes from internal or external environment, which introduce new perceptions, habit of mind and rules of interactions, will not be adapted and particularized to the level at that institution, harmonized with the existent elements of organizational culture.

BIBLIOGRAPHY:

1. ANDRONICEANU, A. *Management public*. Editura Economică. Bucharest. 1999.
2. ANDRONICEANU, A. *Noutăţi în managementul public*, Editura Universitară, 2006.

3. COPELAND, L. & Griggs, L. *Going International*. New York. Plum Books. 1987.
4. DAFT, R.L. Organization: *Theory and Design*, South – Western College Publishing. 2000.
5. DRISKILL, Gerald.W. *Organizational Culture in Action,* Sage Publications, Thousand Oaks, US. 2010.
6. HALL E. T. & Hall Reed, M. Understanding Cultural Differences. Yarmouth: Intercultural Press. 1987.
7. HOFSTEDE, G. *Culture's Consequences: International Differences in Work Related Value*, Sage Publications Inc, Beverly Hills, 1984.
8. HOFSTEDE, Geert, Gert Jan Hofstede & Michael Minkov. *Cultures and Organizations: Software of the Mind*, 3rd Ed. New York: McGraw-Hill. 2010.
9. KLUCKHOHN, F.R.& Strodbeck, F.L. *Variations in Value Orientations*, Row, Peterson & Co, 1961.
10. ONEA, Angelica-Nicoleta. *Diversitate culturală în management: o abordare interregională.* Editura Universităţii "Alexandru Ioan Cuza". Iaşi. 2011.
11. SCHEIN, E. *The Corporate Survival Guide*, San Francisco. Jossey – Bass. 1999.
12. SCHNEIDER, S. & Barsoux, J. L. *Managing Across Cultures*. Prentice Hall. 1997.
13. WILLIAMS, D.& Walters, P. *Changing Culture: New Organizational Approaches*. London. 1989.
14. ONICIUC Corduban, Ionel. The management of individual career in Romanian Army, in the new regional and global security environment. National Defence University "Carol I". Bucharest. 2011.
15. GURGU, Ion. The Professional Human Resources Management of Defence in context of Romanian Armed Forces Reform. Implications over the Romanian Military Art. National Defence University "Carol I". Bucharest. 2007.
16. SMIRCICH, L. *Concepts of Culture and Organizational Analysis. Administrative Science Quarterly*, 1989.
17. SCHEIN, E. *Organizational Culture*. American Psychologist no.45, 1994.
18. http://www.adrnordest.ro/user/file/leader/manual-leadership-in-dezvoltare-regionala.pdf - Agenţia pentru Dezvoltare Regională Nord-Est. Manual de Bune Practici. Leadership în Dezvoltare Regională. 2012.

MILITARY STUDENTS' VALUE ORIENTATIONS

Ludmila VASILACHI
PhD in Pedagogy, University lecturer at the Department Humanistic Science and Foreign language, Military Academy "Alexandru cel Bun", Chişinău, Republic of Moldova.
E-mail address: vasilachiludmila@yahoo.com

Abstract: *The personality value orientation represents the development of self-awareness, assertion of one's own personality and integration in life's values. It is regarded as an element of personality's life strategy and is defined as a tendency to touch and explore a complex of vital goods, important to the personality.*

Peculiarities of the military group, as a specific psychosocial space is defined by a very large influence on the personality of each member of the group being targeted by a variety of beliefs and values that largely depends on the style of cognition and the moral-value level of the person who is the commander of the group and directs the military group's value orientations.

The value system of the military personnel is dominantly oriented to opening, modernity and change and is an important resource of the renewal process both of the military organization and society as a whole.

Namely this fact requires searching and discussion of the psychosocial issues that would ensure the effectiveness of the educational- training process in the Military Academy "Alexandru cel Bun".

Keywords: *the value orientation, particularities of a military group, the value system, the military education environment, personality.*

> "The one who wonders what to do so that his life to make sense, I can answer: "Help Truth, Goodness, Beauty and the Sacred to become alive through your personality! Values are calling for you! They shout for being fulfilled through you. Be, therefore, a creator of values, a carrier of values, a man of value."
>
> *Nicolae Râmbu*[1]

Introduction

The human being's world cannot make sense out of the values and value achievements. The value is an intrinsic part of the social nature of man, without which the human beings could not size the place and his role in the ensemble of the human social life.

To know a man is to know his universe of values. By means of values the man creates his own world incomparable, specific and unique.

1. The issue of value orientation

The value orientation of the personality represents the development of self-awareness, assertion of one's own personality and integration in life's values. It is regarded as an element of self's life strategy and is defined as a tendency to touch and explore a complex of vital

[1] Nicolae RÂMBU, *Philosophy values*, Bucharest, Didactic and Pedagogic Publishing House, 1997, p. 219.

goods, important to the personality. Similarly, the value orientation is a philosophical-ethical and socio-psychological phenomenon which has the function of organizing and regulating the behavior and the content of personality's activity, it forms the human conception of himself and the world. Also in this context it is said that the value orientation characterizes the orientation, directs the human's activity and regulates his social behavior. These are some views that characterize the value orientation as a regulator, but the others treat it through the values.

• The value orientation is the value with major connotation for the personality;

• Axiological orientation represents the value concepts;

• The value orientation is the conscious belief or the subject's representation about what is valuable for him;

The value orientations are often given the same meaning as the beliefs -the product of the later development of the individual. The belief phenomenon means that the disciple has discovered his I and has realized what values were internalized by him. It results that the social directives become beliefs due to a beneficial cognition activity. [2]

The fundamental difference between the world of values and the material world we owe to David Hume. He noted that moral rules are not deducted by the rationality related to the physical world, and, that the difference between vice and virtue cannot be displayed in the material language and the relationships between them. This idea of two worlds is developed by Immanuel Kant in the "Categorical Imperative" of the necessities' world and the world of freedoms. If the world of necessities explored by science then the world of freedoms does not require scientific substantiation. Any attempt to reduce the world of values to the material world is absurd. Of course, it's hard to understand the values' world itself, but focusing only on the physical world, it is impossible. Danish philosopher Kierkegaard S. asks if the honor can replace the hand or foot. And he also says, "It cannot." But it does not follow that honor means nothing. In real life, honor is usually the hidden mechanism of action and its reality emerges when the human being through work and every day effort affirms as a personality and becomes a respected and honored man.

Human beings represent the physical and metaphysical interaction of the matter and spirit, of the sensible and the supersensible, of the determinations and self-reflexes. We cannot imagine a person who does not think himself does not think his thoughts, a man who does not know what he thinks - a consciousness that is not self- conscientious, namely an individual whose existence, like other biological beings, is conducted only in the physical world, of matter.[3]

The soldier, for example, wants to stay alive, but risking his life goes to attack fulfilling his holy duty. Such a behavior regardless of the values cannot be understood.

The values are spiritual, irrational, intuitive, and unconscious. They determine the meaning, direction, strategy of human activity in essence, forming an image of a person's life. Kant wrote that a person proceeds morally not to be happy, but to be worthy of happiness. [4]

The values themselves are outside the context of a rational person. Values do not guarantee the survival of mankind, but without them the existence and development of society is impossible.

The connection between rational knowledge and world of values was observed and explained by Socrates, who emphasized the close connection between truth, good and beautiful. The ability to distinguish between good and evil, beauty and ugliness, nature and

---

[2] Nicolae SILISTRARU, *Values of modern education*, Chişinău, Institute of Education Sciences, 2006, p. 90

[3] Vlad PÂSLARU, *Axiological perspective on education change*, Chişinău, Acad. Of Sciences, Inst. of Education Sciences, Print-Caro, 20011, p. 6.

[4] V.M. SHEMYAKINSKY, *Role of values in shaping world cadet*, Magazine "Teacher Education and Science", 2011, №3. p. 67.

God is not innate or acquired from empirical experience. The human being is susceptible to the world of values not because of his physics, but thanks to spiritual world. If eyes distinguish colors, ears -sounds, the human soul distinguishes the value. Only man reacts to the world of values. Values' world - is a world of freedom. In this world there is a spiritual compulsion which makes it possible for a person to exercise his freedom of choice (to act by circumstances or by conscience).

In determining the contents of education, is very important to choose the system of values. There are many values and all seam important, most of them being proper to all the people, namely are generally human. But any value makes sense only when included in a system.[5]

2. The value orientation in student's military group

Particularities of a military group, as specific psychosocial space, are defined by a very large influence on the personality of each member of the group being targeted by a variety of beliefs and values that largely depend on the cognitive style and moral- value level of the person performing the function of the group commander and who directs the military group's value orientations.

The value system of the military personnel is dominantly oriented to opening, modernity and change and is an important resource of the renewal process both of the military organization and society as a whole.

Thus, the value system that guides the military attitude towards work consists of: discipline, sense of responsibility, honesty, dignity, honor, loyalty to the military institution, concern for improvement and personal example. [6]

It is clear that the military education environment is different from the rest of the educational activity, so we can mention special characteristics of the military system, such as: limiting the freedom of action on the behalf of the institution, the often teams work spirit, professional demands with novelty character, inter-human relations based exclusively on the hierarchy and the help each other spirit, statuses and roles covered express, the own code of behavior different from the civil one by stringency, specific communication system and moral values, activities with a high degree of physical and mental demand, risk-taking, strictly managed and controlled life and work style, participation in high-risk and life-threatening missions, studying the complexity of military equipment and weapons. [7]

We can mention that the value orientations system in the group of military students is influenced by different factors and components:

I. The military value and attitudes orientations, as a style of behavior, of moral values and as well as the "military honor", responsibility for the country, manifested in the military rituals and traditions as a stimulus for initial forming and service training in the process of the military education. These desideratum lead to the idea that:

- currently the young soldiers continue the family tradition even being in the military service;
- engage in further military traditions of the Army in strict accordance with the honor and dignity of a military officer;

[5] Nicolae SILISTRARU, *Values of modern education*, Chişinău, Institute of Education Sciences, 2006, p. 63.
[6] Claudiu NICULAE*., Military values - resources integration into NATO*. Sociology Romanian, Bucharest: 1-4, 2001, p. 124-133.
[7] Elena DUMITRU, *Values of military education today*, In: Area Southeast European globalization, Scientific Session with International Participation, Strategies XXI, April 12 to 13, 2007, Bucharest: "Carol I" National Defence University, 2007, p.171.

- develop the increased sense of personal involvement and responsibility for the fate and security of the country;
- enforce the respect for personal discipline and military;
- create a desire to be in the bosom of the military staff to train in "military camaraderie."

II. The group of professional military value orientations that contribute to the formation of the military attitudes specific to students from the military institutions are:

- the quality of acquiring the knowledge in the military field;
- the desire to work in a favorite military specialty;
- the desire to handle all types of small arms;
- the desire to learn to work in complex modern weapons systems and automated control systems;
- the desire to master skills of driving the military equipment;
- the need for professional self-organization;
- the desire to make a good career in the military system;
- the desire to acquire unique skills;
- the desire for physical perfection (acquisition of skills in martial arts).

III. The group of cognitive development of the students' value orientations that promote the formation of the following states:

- the desire of creativity and ability to draw a parallel with civilian life (psychology, pedagogy, etc.).
- the wish to test, in difficult and specific living conditions the professional activities;
- the desire to see life in different regions of the world;
- the desire and ability to acquire basic knowledge on a wide range of disciplines, from exact (mathematics, physics), to the humanity ones (sociology, psychology, philosophy);
- the desire to communicate with interesting people with huge experience in service, engaged in various situations.

IV. Value orientations and group attitudes specific mercantile type and active social position in society:

- the desire to acquire, during service in the armed forces, skills and knowledge necessary for daily life;
- obtaining specific benefits and advantages for their lives during military service;
- fight for financial autonomy and personal independence;
- getting free education oriented to prestige of undergraduate degree;
- the desire to make a military career to achieve a certain status in the society.

V. Group value orientations and attitudes towards leading a decent life:

- regardless of the economic crisis, the remuneration is guaranteed;
- the desire to provide his family financial right, including the housing insurance;
- the desire to live in dignity, with a dignified status in the society.

It should be mentioned that the military education environment is based also on a highly formalized system; it operates with specific sets of sanctions, and the performance of the group members dependent on the prestige of formal leaders.

These features represent a value system specific to the education in the military institutions.

In order to elucidate the value orientations in military activities, the students have been given the survey containing the necessary values of a military officer.

1. Courage, daring.
2. Leadership spirit.
3. Quick Decision, spontaneity.
4. Energy, perseverance.
5. Cold Blood, hold power.
6. Strength of character.
7. Spirit of order.
8. Devotion.
9. Good comrade.
10. Virtuous.
11. General Intelligence.
12. Practicality.
13. Willing to perfection.
14. Honesty and morality.
15. Physical Health.
16. Good educator.
17. Spirit of the organizer.
18. Effectiveness in action.
19. Independence.
20. Originality

The investigation took place in the following way: the students of the IV-th year of study, Infantry platoons, artillery and signals were offered a list of values in the survey above. Asked what would be three values that they believe are dominant in the work of a commander (with a choice of 20, and having the opportunity to express their points of view to the value unspecified). Each of them chose firstly the value that he believes dominant for the profession of an officer and wrote it on a piece of paper with rank 1 (one) for classification, then the value he believes that occupies the second rank and so on, until he will complement the whole survey.

The survey results were:

The first three values are dominant in the profession of officer:

- Leader spirit ;
- Energy, perseverance, diligence;
- General Intelligence,

Reasons for the three dominant values should be taken are:

- Officer leadership required greater than any other professional because the officer activates both the educator and the command line. As an educator, he makes people's education and military training, and as commander leads his subordinates.

Officer- Commander must have the following characteristics:

a) Have provided, in the sense of physical appearance, which requires the order;
b) Have good voice control; is vigorously
c) Be familiar military art and science;
d) Will have to be always perfect, both in terms of military knowledge and their practice;
e) To treat human soldiers, to earn while prestige, which should enjoy a true master.

- Energy is needed both to rule the people command line and if military action because it underpins military leadership. Officer is also required to be persistent and diligent man, because he gets the job usually multiple and diverse missions, to be followed over time and often executed.

- As the officer has to fulfill multiple and varied tasks within his profession, he is required to be intelligent, so to be able to cope with educational, technical and tactical problems, the solution of which is not always known in advance, everything depend on the decision that the commander will take, even human lives.

Conclusion

Referring to the major significance of education in the Military Academy "Alexandru cel Bun" remains to be that of training and the complex modeling of future officer – a competitive well-trained specialist, who is able to cope with difficult situations he will face both on professional and social level.

From this perspective, I would mention the following proposals:

– In any activity, concentrated values at the level of correlation between outcomes and general contents to continue a unique criterion of the military students' education;

– Designing the teaching activities of military students' axiological forming to take into consideration the specific features of this group;

– The main valued subject of the educational actions in the mentioned institution will still remains the personality (teacher, commander, military officer, sergeant, etc.) that teaches through personal example.

BIBLIOGRAPHY:

1. NICULAE Claudiu, *Military values - resources integration into NATO*. In: Sociology Romanian, Bucharest, 1-4, 2001, p. 124-133.
2. DUMITRU Elena, *Values of military education today*, In: Area Southeast European globalization. Scientific Session with International Participation. Strategies XXI, April 12 to 13, 2007, Bucharest, National Defense University "Carol I", 2007, p. 164-177.
3. PÂSLARU Vlad, *Axiological perspective on education change*, Chişinău, Acad. Of Sciences, Inst. of Education Sciences, Print-Caro, 2011.
4. RÂMBU Nicolae*, Philosophy values,* Bucharest, Didactic and Pedagogic Publishing House, 1997.
5. SILISTRARU Nicolae, *Values of modern education*, Chişinău, Institute of Education Sciences, 2006.
6. SHEMYAKINSKY Viktor M.*, Role of values in shaping world*, Cadet Magazine "Teacher Education and Science", 2011, №3.

INCREASING MANAGERIAL ACTIVITY IN ORDER TO ELIMINATE PAYMENT DIFFERENCES IN RELATION TO THE ARMED FORCES OF THE NORTH-ATLANTIC TREATY ORGANIZATION AND THE EUROPEAN UNION

Ion VASILE
PhD in Military Sciences, "Carol I" National Defence University, Bucharest, Romania.
E-mail address: vasileion1962@yahoo.ro; ivasile@mapn.ro

Abstract: *One of the objectives of the Governing Programme for 2013-2016[1], laid down in the chapter entitled "Defence", stipulates "the revision of the normative framework specific of defence, military career management and the system of occupational pensions for the military". Another course of action is focused on "improving the life quality of the Romanian Armed Forces personnel, in keeping with the domestic economic and social environment, as well as Romania's NATO and EU member status, while raising the attractiveness of the military profession".*

The revision of the normative framework specific of defence may start from analyzing and correlating the Romanian payment system and the systems implemented in the NATO and EU member states, by eliminating payment differences. A well-determined financial decision, sustained by flexible and modern financial management is the fundamental act that may contribute to attaining this objective, especially within the context of the latest security events in the region, given Romania's commitment to contribute to the development of the Allied capabilities.

Keywords: *unitary payment system, military pay, salary, management.*

Introduction

The present approach is largely based on the results of the professional activities meant to ensure the regulation, implementation, methodological coordination, specialized assistance and evaluation of the current payment system for the Ministry of Defence personnel, as well as the activity of documenting, monitoring and analyzing the payment systems implemented in the armed forces of the NATO and EU member states.

The military forces have a distinct identity in society. Stephen R. Covey[2] claims that effective interdependence can only be built by relying on real interdependence. Therefore, I consider that society, with all its components, must understand it is inter-conditioned with the Romanian military: the way the military institution manifests respect towards society should be reflected in the amount of payment for the military personnel.

With a view to achieving a modern, professionalized, deployable, sustainable, flexible and mobile force structure, with a high potential of action in a large range of missions both on the national territory and outside it, I consider that, together with the continuation of the military institution's adaptation process, it is imperative to have as

[1] *Programul de Guvernare 2013-2016 (Governing Programme for 2013-2016)*, published in Monitorul Oficial al României, Part I, No. 877/21 December 2012.
[2] Stephen R. COVEY, *Cele 7 deprinderi ale persoanelor eficace*, Allfa Publishing House, Bucharest, 2011, p. 171.

primary objective the elimination of payment differences in relation to the armed forces of the NATO and EU member states.

1.Data regarding personnel payment in the Romanian budget sector

After the collapse of the communist system, Romania faced considerably higher inequality in the distribution of personnel incomes.

The proportion of salaries in the population's overall income diminished.

It is a well-known fact that, between 1990-2009, occasional changes took place in the budget sector at the level of base salaries, which were raised only for the personnel from certain fields of activity.

Framework law no. 284/2010 on the unitary payment of the personnel paid from public funds[3] with subsequent alterations, proposes a new payment system for the personnel paid from public funds, a new and coherent way of position hierarchy, a new and unitary legislative outlook on a long and medium term.

The framework law on the unitary payment of the personnel paid from public funds is focused on the conversion from non-homogeneous salary systems to a unitary one for the personnel paid from public funds.

The framework law on the unitary payment of personnel paid from public funds was meant to establish a 1 to 15 ratio between the minimum base salary – equal to the minimum gross base salary guaranteed as payment[4] - and the maximum one, so as to limit the number of salary categories to 110 and to limit salary increases, compensations, bonuses, individual indemnities to maximum 30% from the base salary, salary/military pay for the basic position or monthly employment indemnity.

However, because of the financial constraints, the salaries and military pay of the personnel from the budget sector paid from the state general consolidated budget could not be established according to this law; therefore, the same imbalances persist, with a 1-35 imbalance between the minimum and the maximum base salary.

The salary system for personnel paid from public funds, proposed by Framework law 284/2010 with subsequent alterations focuses on establishing the function pay and base salaries by multiplying the hierarchy coefficients corresponding to the salary categories by the reference value represented by the minimum gross base salary per country guaranteed as payment.

In my estimation, the framework law on the unitary payment of personnel paid from public funds is the normative act that can thoroughly, objectively and rationally ensure the eradication of salary discrimination in the budget sector. I am positive that, by establishing the base salaries and function pays by multiplying hierarchy coefficients by the value of the minimum gross base salary per country guaranteed as payment,

---

[3] *Legea nr. 284/2010 privind salarizarea unitară a personalului plătit din fonduri publice (Framework law No. 284/2010 on the unitary payment for personnel paid from public funds)*, published in Monitorul Oficial al României, Part I, No. 877/28 December 2010, with subsequent alterations.

[4] According to Art. 164, Par. (1) from *Legea nr. 53/2003 – Codul muncii (Framework law No. 53/2003 - the Labour Code)*, published in Monitorul Oficial al României, Part I, No. 345/18 May 2011 with subsequent alterations and completions, the minimum gross base salary per country guaranteed as payment is established by Government decision. According to *HG nr. 871/2013 pentru stabilirea salariului de bază minim brut pe ţară garantat în plată (Government Decision No. 871/2013 for establishing the minimum gross base salary per country guaranteed as payment)* published in Monitorul Oficial al României, Part I, No. 703/15 November 2013, beginning with 1 January 2014, the minimum gross base salary per country guaranteed as payment will be 850 lei (191 Euros) and, beginning with 1 July 2014, the minimum gross base salary per country guaranteed as payment will be 900 lei (202 Euros).

representing the reference value, there will be no more discrepancies in the social hierarchy of payment for personnel from the budget sector.

In my opinion, politically speaking, the solution of maintaining the gross quantum of base salaries and function pays from December 2009, as has been the case since 1 December 2012 to this day, should not have been adopted.

I support the idea that it is necessary to calculate base salaries, function pays and monthly employment indemnities by multiplying the hierarchy coefficients by the reference value equal to the minimum gross base salary per country guaranteed as payment, while limiting the amount of this „fixed" salary element. The upper limit of the monthly quantum for gross base salaries, function pays and monthly employment indemnities may be stipulated for together with the hierarchy coefficients corresponding to the salary categories established in Art. 10, Par. (2) from Framework-law No. 284/2010 with subsequent alterations.

Likewise, there is the possibility of establishing the reference value at an acceptable level, in keeping with the budget constraints; for instance, during the gradual enforcement of the framework law on the unitary payment for personnel paid from public funds, started in 2011, the reference value could have been half of the minimum gross base salary per country guaranteed as payment.

In my opinion, an increasing managerial activity meant to eliminate payment differences in relation to the armed forces of the NATO and EU member countries must take into account that the current components of the unitary payment system – generated by problems occurred in payment practice. For the Ministry of Defence these subsystems are the following: salary rights, made up of two elements: the fixed part, comprising the basic function pay, that is the base salary, and the variable part, made up of additional salary rights; advantages or facilities in kind; money benefits; social compensations; budgetary salary obligations; establishing the amount of money rights and sums owed to third parts; transferring receivables and, if this is the case, of salary deductions; paying the net salary earnings; declaring the insured personnel; monitoring and controlling the enforcement of regulations; working out and planning the necessary funds for personnel expenditures.

A specific feature of Framework law No. 284/2010 with subsequent alterations is that it is the result of an ample analysis and construction project, in cooperation with Romanian[5] and World Bank expert groups.

In our view, it is recommendable that, starting with 1 January 2015, base salaries and function pays, as well as monthly employment indemnities should be calculated by multiplying the hierarchy coefficients stipulated in Framework law No. 284/2010 with subsequent alterations by the reference value equal to the minimum gross base salary per country guaranteed as payment. This is a daring statement – some might even deem it surprising and unbelievable. To sum up, the salary policy promoted by the political-strategic factor must be in agreement with the current legislative framework and the evolutions of the domestic and international environment, but the fiscal and budgetary measures within the reference area must boost economic efficiency by raising the salary rights.

[5] The bipartite commission was created by *Ordinul nr. 1774 / 2009 al ministrului Muncii, Familiei şi Protecţiei Sociale (Order of the minister of Labour, Family, Social Protection and Elderly No. 1.774/2009)*; later on, the composition of the bipartite commission was updated by Orders of the minister of Labour, Family, Social Protection and Elderly No. 318/2010 and 433/2010. The author of this approach represented the interests of the Ministry of National Defense within the bipartite commission.

2. Aspects regarding the payment of the military personnel in the Romanian Armed Forces and in the NATO and EU member states

Comparing the regulations in the NATO and EU member countries to the national ones, we may conclude that between the European provisions and those that regulate the unitary salary system in Romania there are similarities and differences. We consider that it is necessary to gradually introduce in the Romanian unitary payment system those particular norms stipulated in the NATO and EU member states' legislation.

Starting from the experience accumulated in dealing with salaries and pensions, I deem that the general economic decline, generated by the world economic crisis, represents the main cause of the salary differences in relation to the NATO and EU member states' armed forces. Up to a certain point, this difference in monthly individual gross pay may be deemed normal within the context of Romania's transition from a centralized economy, with a labour market strictly controlled by the state, outside the action of market mechanisms, to a market economy, with a liberalized labour market. However, salary inequities – as long as they are largely caused by economic factors – are the result of a power capable of producing not only inequality but also inequity.

We discover that salary imbalances and inequities have continued to proliferate in the last years, although, by implementing the provisions of Framework law No. 284/2010 with subsequent alterations in 2011, the Government acquired highly functional salary policy levers.

The salary policy represents one of the important tools with which the modern state shapes both its economic and social policy. The salary policy for the personnel paid from public funds is promoted in keeping with the fiscal and budgetary measures to be implemented in the reference area, as established by the Government's fiscal-budgetary strategy.

Cezar Corneliu Manda[6] considers that "every analysis must by all means start from an introspection of the state, the omnipresent subject, dominant in the social-political, economic and juridical life of every nation and implicitly of its citizens". The state is "such a strong and living authority that is absorbs everybody's individuality."

We notice that for Romania in 2014 the personnel's payment continues to be the core of the problem for political decision-makers. For this year, the nominal upper limit of the personnel expenditures pertaining to the general consolidated budget[7] is set at 47,8 billion lei, respectively 7,3% of the gross domestic product.

Starting from the remark that, by its economic and fiscal policies, the state may intervene to eliminate salary differences in relation to the armed forces of the NATO and EU member states, we reiterate that, at the present moment, the payment of the salary rights for the military and civilian personnel paid from public funds is provided according to the provisions of Framework law No. 284/2010 with subsequent alterations, the special annual

---

[6] Cezar Corneliu MANDA, *Teoria administraţiei publice*, C. H. Beck Publishng House, Bucharest, 2013, p. 1.

[7] According to Art.1 Par. (2) and Art. 2, point 7 from *Legea nr. 500/2002 privind finanţele publice (Law No. 500/2002 on public finances)*, published in Monitorul Oficial al României, Part I, No. 597/13 August 2002 with subsequent alterations and completions, the law of finances defines the syntagm „general consolidated budget" as follows: the sum of all budgets (state budget, state insurance budget, budget for special funds, budget for the state treasury, budget for autonomous public institutions, budget for public institutions integrally or partially financed from the state budget, budget for the social state insurance and, if this is the case, budgets for public institutions integrally financed from own incomes, budget for funds from external credits concluded and guaranteed by the state, whose reimbursement, interests and other costs are provided from public funds and budget for external non-reimbursable funds, components of the budget system, corroborated and consolidated into a whole.

law[8] and, in keeping with the limits imposed by the financial resources, approved for the Ministry of National Defence by the annual budget law[9] under the heading „personnel expenditures"[10].

We discover that in the budget year 2014, the average gross individual monthly pay[11] is as follows: for active military personnel from the officers' category - 4.370 lei (982 Euros); for active military personnel from the NCOs' and warrant officers' category - 2.086 lei (469 Euros); for active military personnel - 2.884 lei (648 Euros); for active soldiers and NCOs - 1.214 lei (273 Euros). Therefore, for the active military personnel the average gross individual monthly pay is around 2.165 lei (487 Euros).

Next we will present some minimum monthly salaries, expressed in Euros, from the NATO-EU member states, in keeping with the data provided by the EU Statistics Office - Eurostat: Belgium - 1.501, Bulgaria – 158, the Czech Republic – 312, Croatia – 374, Estonia – 320, France – 1.430, Greece – 683, Ireland – 1.461, Latvia – 287, Lithuania – 289, Luxembourg- 1.874, Malta – 697, Great Britain – 1.264, Netherlands – 1.469, Poland – 376, Portugal – 565, Slovakia – 337, Slovenia – 783, Spain – 752, Turkey – 428, Hungary – 340.

We estimate that, in approaching the main elements of the salary system for the military personnel in the Romanian armed forces and the armed forces of the NATO and EU member states, it is useful to point out that in Germany, France, Austria, the Czech Republic and others we find laws which regulate the setting-up of a unitary payment system for the budgetary personnel paid from the state general consolidated budget. At the same time, we must emphasize that states such as Belgium, Bulgaria, Italy, the Netherlands, Slovakia, Spain and the USA have special payment laws for the military personnel from their armed forces.

As is known, between the resources necessary for the military institution to ensure forces capable of protecting the national interests and values and the real resources allotted to this effect there is a fundamental contradiction, engendered by the growing discrepancy between necessities and what can be concretely allocated. In my estimation, it is imperative to reach a balance between the need to protect the national interests in the field of defence and the resources that can be really allotted to this effect.

---

[8] According to Art. 7, Par. (1) from *Framework law No. 284/2010* with subsequent alterations, "the implementation of the provisions of this law is to be gradual, by successive modifications of the base salaries, basic function pays/basic function salaries and monthly employment indemnities by special annual enforcement laws". The special annual enforcement law for 2014 is the *OUG nr. 103/2013 privind salarizarea personalului plătit din fonduri publice în anul 2014, precum şi alte măsuri în domeniul cheltuielilor publice (Government's Emergency Ordinance No. 103/2013 on the payment for personnel paid from public funds in 2014)*, as well as other measures in the field of public expenses, published in Monitorul Oficial al României, Part I, No. 703/15 November 2013. In my opinion, the current calculation algorithm for salary rights does not favour competition and individual development.

[9] According to *Law No. 500/2002 on public finances*, published in Monitorul Oficial al României, Part I, No. 597/13 August 2002 with subsequent alterations and completions, the annual budget law is the law that stipulates and authorizes incomes and budget expenses for each year, as well as regulations specific of the budget year; for the financial year 2014 the budget is approved by *Legea nr. 356/2013 a bugetului de stat pe anul 2014 (State Budget Law No. 356/2013 for 2014)*, published in Monitorul Oficial al României, Part I, No. 805/19 December 2013.

[10] *Legea nr. 69/2010 – Legea responsabilităţii fiscal-bugetare (The law for fiscal-budgetary responsibility No. 69/2010)*, published in Monitorul Oficial al României, Part I, No. 252/20 April 2010 with subsequent alterations and completions, defines personnel expenses as follows: the overall expenses from the general consolidated budget during a budget year in relation to the civilian and military budgetary personnel, public dignities with any kind of remuneration, such as employment salary or indemnity, other benefits, including additional payments, incentives, rises, extra hours and other benefits of any kind, as well as contributions to the budget of state social insurance and the related budgets for special funds.

[11] The average leu-euro ratio for 2014 is 4.45 lei, according to the *fiscal-budgetary strategy for 2014-2016*, issued by the Romanian Government.

3. A modality of approaching the problem range linked to an increasing managerial activity with a view to eliminating salary differences in relation to the armed forces of the NATO and EU member states

The leu/euro curs has risen from 3,1 lei in 2007 to 4,5 lei this year. Romania has officially notified the European Commission that it will adopt the euro currency starting with 2019.

In this situation, I estimate it necessary to appreciate the leu in relation to the euro – a tendency encouraged by the National Bank of Romania – in the years preceding the transition to the euro currency. Obviously, this rise of the leu can be achieved within a positive global context (for example, without new important corrections in the stock exchange and unless the important economies get – again - into recession).

I consider that, in the new economic conditions, the work relations between the military personnel and the military institution become „partnership relationships", capable of generating the highest performance level in the Romanian Armed Forces. „It is about people working together to fulfill certain common objectives."[12] In my estimation, the key points in a successful „partnership relationship" are the following: mutual benefits, confidence, long-term perspectives, excellencies, competence, „open" communication, mutual influence and assistance, „day-to-day" behavior, equitable remuneration. Since commanders and higher-in-rank differ by what they do with their authority, the personnel reacts well when the authority is used beneficially, taking into account the key points in the successful „partnership relationship" mentioned above.

This approach is also found in "Fundamentele managementului organizaţiei"[13]: „The quality of managerial solutions and, implicitly, the functionality and performances of the organization strictly depend on its managers and leaders. Their contribution to establishing and fulfilling the objectives is – obviously, without substituting themselves to the work of other categories of personnel – often decisive."

At the same time, I support the idea that the national salary policy is influenced by Romania's double status as a NATO and EU member state.

Likewise, I consider that eliminating salary differences in respect to NATO and EU member states will imply continuing the efforts of revising the force structure in order to generate highly sustainable and interoperable capabilities: flexible, mobile, rapidly deployable, capable of participating in the whole range of international missions.

I suggest the objectives, courses of action and priorities meant to eliminate salary differences as compared to the armed forces of the NATO and EU member states and to guide the activity of the Ministry of Defence should be stipulated for in the „Strategy for improving the salary system for the personnel of the Romanian Armed Forces", included in the „Programme for raising the military pay for professional military personnel between 2015-2020" and in the „Multi-annual plan for eliminating salary differences as compared to the armed forces from NATO and EU member states for 2015-2020".

At the same time, another measure that could be implemented, a first for the budget personnel paid from the state general consolidated budget, is to set up a „Remuneration Committee" – a totally independent structure, which will evaluate and monitor the Government's salary policy, as well as the managerial activity, with a view to eliminating salary differences in relation to the armed forces of NATO-EU member states. It is useful for this committee to be made up of five members (none of them employed in the budget sector,

[12] David SIROTA, Louis A. MISCHKIND, Michael Irwin MELTZER, *Motivarea angajaţilor. Cum creşte performanţa companiei odată cu entuziasmul oamenilor*, ALL Publishing House, Bucharest, 2010, p. 270.
[13] Ovidiu NICOLESCU, Ion VERBONCU, *Fundamentele managementului organizaţiei*, Universitară Publishing House, Bucharest, 2008, p. 366.

which will ensure total impartiality in evaluating the Government's salary policy and the managerial activity of the Ministry of Defence).

The „Remuneration Committee" may lay on western basis the whole salary system of the Romanian Armed Forces personnel, which will be evaluated according to certain well-established criteria, meant to clearly show the ratio between the gross individual monthly pay and the responsibility per active military man, thus helping us to make it realistic and optimize it.

Also, in my opinion, to ensure the programme and planning management mentioned above and to fulfil the tasks incumbent on the military institution, a „financial-accounting committee" must be set up, where the minister of defence will have a consulting role, as the main budget manager; I have in view the fact that, in keeping with Art. 6, Par. (1) from Framework law No. 284/2010 with subsequent alterations, „the management of the payment system for the personnel [...] is ensured by each main budget manager". I estimate that the activities of this committee will focus on providing assistance and counselling to the minister of national defence, politically committed to eliminate salary differences in respect to the armed forces of the NATO-EU member states. The financial-accounting committee of the Ministry of Defence must analyse the situation of payment for the military and civilian personnel, base its decisions on studies and analyses made by the Financial-Accounting Directorate, draw up a report to be presented to the Ministry of Defence College and make suggestions regarding the payment for next year (its organization and functioning being decided by order of the minister of defence).

Additionally, I consider it useful to set up a „Commission for revising the incomes of the Romanian Armed Forces personnel". Actually, the possibility of salary rises for the military and civilian personnel is constantly focused on by the Financial Accounting Directorate; this involves a thorough analysis and hard work by a team of specialists, economists from the Financial Accounting Directorate, Human Resources Management Directorate, together with military law specialists and other professionals with experience in this field.

I suggest the following concrete and measurable salary rights:

a) granting bonifications for dangerous, harmful or hard work conditions, in a fixed amount, determined in relation to the minimum gross salary guaranteed as payment;

b) granting a monthly bonification (calculated by applying a percentage to the average gross salary earnings used to calculate the state social insurance budget[14]) for personnel who have performed the tasks pertaining to their positions for more than four years (starting with the date mentioned in the assignment order), as follows: in the 5th year: 10%; in the 6th year: 20%; in the 7th year: 30%; in the 8th year: 40%; over 9 years: 50%;

c) granting a monthly bonification for military service, amounting to 1% from the average gross salary earnings used to calculate the state social insurance budget, for each seniority year of military service;

d) granting a bonification for rank seniority;

e) granting a special money reward in the last month of each trimester for fidelity to the country and in service of the nation, equal to the minimum gross salary guaranteed as payment;

f) granting a monthly reward in exchange for the specific constraints involved by the military career (for example, interdiction or restriction on certain rights and liberties stipulated

[14] The average gross salary earnings used to calculate the state social insurance budget for 2014 is 2.298 lei (516 Euros), according to Art. 16 from the *Legea nr. 340/2013 - Legea bugetului asigurărilor sociale de stat pe anul 2014 (Law for the social insurance budget for 2014 No. 340/2013)*, published in Monitorul Oficial al României, Part I, No. 776/12 December 2013.

for in the Romanian Constitution), amounting to 50% of the minimum gross salary guaranteed as payment;

g) awarding yearly, in December of each budget year, a professional performance indemnity, according to the funds available for personnel expenditures;

h) granting a family bonus to the active military personnel moved to a different location, over 250 km from the residential one, to compensate for family separation;

i) allotting a sum of money, apart from the gross individual monthly pay, for the holiday period, in May of each budget year;

j) granting rewards for performing extraordinary work tasks (for instance, assistance in case of natural calamities, atmospheric - climate change, drought, hurricanes, snow and ice, storms, tornadoes, fires – and geological – earthquakes, floods, land slides, tsunamis, volcanoes);

k) total or partial reimbursement of costs associated with the possession and use of the private phone and the internet – the equivalent in lei of 100 Euros being the upper limit – to the military personnel participating in missions in the theatres of operations outside the Romanian territory, according to the necessities of the Ministry of National Defence, in order to meet the obligations assumed by Romania in international conventions and treaties;

l) granting an efficiency indemnity to the military personnel participating in missions in the theatres of operations;

m) granting fiscal discounts to the military personnel participating in missions in the theatres of operations;

n) exemption from certain local taxes for military who accomplished missions in theatres of operations;

o) granting a compensatory allocation for establishing the daily quantum of the monthly pay in relation to the number of calendar days for each month of the year;

p) granting an exceptional bonus to the military personnel that are rated „exceptional" in their yearly work records.

I also recommend reducing the number of tertiary budget managers[15] and financial-accounting departments[16] in the Romanian Armed Forces, while setting up a few territorial payment and fiscality-salary income offices, methodologically coordinated by a centre subordinated to the Financial-Accounting Directorate[17], as well as the organization and functioning of the military fiscal body, subordinated to the Financial Accounting Directorate and methodologically coordinated by the National Agency for Fiscal Administration.

In conclusion, in order to fulfil the tasks incumbent on the military institution, I propose drawing up the necessary planning documents to eliminate salary differences in relation to the armed forces of the NATO-EU member states. I estimate that the Ministry of Defence must set in agreement the legislative-normative framework and the national and international political, economic, social and military evolutions by: creating the conditions for drawing up

[15] According to *Law No. 500/2002 on public finances*, with subsequent alterations and completions, the heads of public institutions with legal personality (in our case, the commanders of military units) subordinated to the main budget manager (more specifically, the minister of national defense) are secondary or tertiary budget managers, as is the case. Tertiary budget managers use the budget credits allotted to them only for fulfilling the tasks of the institutions they are in charge of, in keeping with the provisions of the approved budgets and the conditions established by legal provisions.

[16] According to *Law No. 500/2002 on public finances*, with subsequent alterations and completions, the financial-accounting department represents the organizational structure of a public institution, which organizes budget execution (service, office, department).

[17] According to Art. 17 from *Legea nr. 346/2006 privind organizarea şi funcţionarea Ministerului Apărării Naţionale (Law No. 346/2006 on the organization and functioning of the Ministry of National Defense)*, published in Monitorul Oficial al României, Part I, No. 654/28 July 2006 with subsequent alterations, the Financial Accounting Directorate is responsible for accomplishing the financial accounting duties incumbent on the minister of National Defense as main budget manager.

a Government decision in agreement with the provisions of Art. 32 from Appendix No. VII of Framework law No. 284/2010 with subsequent alterations („The Romanian government is also entitled to establish other salary rights specific of the personnel from public defence institutions, public order and national security, upon proposals made by their leaders"); perfecting the Statute of the military personnel; drawing up the „Strategy for perfecting the payment system for personnel working in the Romanian Armed Forces", the „Programme for raising the payment of professional military personnel between 2015-2020", „Multiannual plan for eliminating payment differences in relation to the armed forces of the NATO-EU member states between 2015-2020", and, last but not least, defining the political-military ambition level of the Romanian Armed Forces.

Conclusions

As George Cristian Maior[18] points out, „It is clear that we are living in a century full of uncertainty, therefore, with a high potential for unpredictability and unknown as to the new challenges we will have to face or the threats we are and will be confronted with from now on. This must not discourage us from finding the necessary answers to more and more difficult questions."

The basic element in payment is the motivation of the military personnel. I consider that the military institution has undergone thorough changes; by attracting human resources that meet the quantitative and qualitative requirements for creating professional armed forces, renewing human resources and professionalizing the personnel, the mentality of the Romanian Armed Forces has changed.

Thus, for services performed by the Romanian military forces expected to be professional by international standards even at the price of the supreme sacrifice, it is desirable that the decision-makers should also pay adequate salaries.

The status of military in the armed forces of a NATO-EU member state implies a salary system in keeping with the activity performed in service of the country, for promoting the values of democracy and civilization, while eliminating the payment differences in relation to the armed forces of NATO-EU member states.

In order to accomplish the specific objectives in eliminating the payment differences in relation to the armed forces of the NATO-EU member countries, we must do our best to answer several questions.

The theoretical and practical applicability is provided by the „Strategy for perfecting the payment system for personnel working in the Romanian Armed Forces", the „Programme for increasing the payment of professional military personnel between 2015-2020", the „Multi-annual plan for eliminating payment differences in relation to the armed forces of the NATO-EU member states between 2015-2020".

I consider that the responsible authorities in Romania should manifest deeper interest regarding the elimination of payment differences in relation to the armed forces of NATO-EU member states.

BIBLIOGRAPHY:

1. Law No. 500/20023 on public finances, with subsequent alterations and completions.
2. Law No. 53/2003 – Labour Code, republished, with subsequent alterations and completions.

[18] George Cristian MAIOR, *Incertitudine. Gândire strategică şi relaţii internaţionale în secolul XXI*, RAO International Publishing Company, Bucharest, 2009, p. 24.

3. Law No. 346/2006 on the organization and functioning of the Ministry of National Defence, with subsequent alterations.
4. Framework law No. 284/2010 on the unitary payment of personnel paid from public funds, with subsequent alterations.
5. The Law for fiscal-budgetary responsibility No. 69/2010, with subsequent alterations and completions.
6. The Law of state social insurance budget for 2014 No. 340/2013.
7. The Law of state budget for 2014 No. 356/2013.
8. Government's Emergency Ordinance No. 103/2013 on the salary of personnel paid from public funds for 2014, as well as other measures in the domain of public expenses.
9. Government Decision No. 871/2013 for establishing the minimum gross base salary per country guaranteed as payment.
10. Order of the minister of Labour, Family, Social Protection and Elderly No. 1.774/2009 and Orders of the minister of Labour, Family, Social Protection and Elderly No. 318/2010, 396/2010, and 433/2010.
11. Governing Programme 2013-2016, published in Monitorul Oficial al României, Part I, No. 877/21 December 2012.
12. The fiscal-budgetary strategy for 2014-2016 issued by the Romanian Government
13. MAIOR, George Cristian, *Incertitudine. Gândire strategică şi relaţii internaţionale în secolul XXI*, Editura RAO International Publishing Company, Bucharest, 2009.
14. MANDA, Cezar Corneliu, *Teoria administraţiei publice*, Editura C. H. Beck, Bucharest, 2013.
15. NICOLESCU, Ovidiu; Ion Verboncu, *Fundamentele managementului organizaţiei*, Editura Universitară, Bucharest, 2008.
16. COVEY Stephen R., *Cele 7 deprinderi ale persoanelor eficace*, Editura Allfa, Bucharest, 2011.
17. SIROTA, David; Louis A. MISCHKIND, Michael Irwin MELTZER, *Motivarea angajaţilor. Cum creşte performanţa companiei odată cu entuziasmul oamenilor*, Editura ALL, Bucharest, 2010.

ROMANIAN PARTICIPATION IN PROJECTS DEVELOPED WITHIN SMART DEFENCE INITIATIVE

Robert-Mihai POENARU
PhD candidate in Military Science and Information within
"Carol I" National Defence University, Bucharest, Romania; founding member
of the "Centre for Security Studies, Crisis Management and Conflict Prevention".
E-mail address: poe_robert87@yahoo.com

Abstract: The appearance of new threats to global security, and especially to the Euro-Atlantic area could not leave indifferent the main organization involved in ensuring this security. Once the idea that in way to have a more secure Euro-Atlantic space, the organization has to take the fight against terrorism beyond the conventional barriers, was understood by the NATO leaders, the Alliance has become more powerful.

Due to the global economic crisis NATO created a new initiative, Smart Defence, which seeks to develop new capabilities and to maintain the current ones at a maximum capacity. Each member country has its own security culture, its habits, laws and their concepts in terms of security, but it is understood that through the development of this concept we can create a more powerful force, a flexible one, a force that will always be ready for intervention where the Alliance will consider it is necessary.

Given Romania's economic possibilities, taking into account here the low percentage that was assigned to the Ministry of National Defence in the past years, without taking into account the commitments that were made by our country at the international level, we believe that Romania can find in this concept a viable solution to existing problems.

Keywords: Smart Defence, global security, NATO new concept, new capabilities, Romania and Smart Defence

In these times when NATO faces problems caused by changes in the global security environment and the emergence of new threats, the Allies must find new solutions to provide the security of the Euro-Atlantic area. From its foundation until now, the Alliance managed to resist and face all the threats that came against it. We have to appreciate especially the extremely effective way in which NATO managed to realigned its goals, created new strategies and managed to adapt to new challenges.

The new challenges faced by the Alliance in these moments are given by the emergence of the economic crisis, by the emergence of new state actors who wish to have a more important role both regionally and globally (e.g. Russia, China, India, Brazil) and by the crisis in the Ukraine, a state located close to the borders of the Alliance, which in case it would fall under the influence of Russia, can create tension and a state of major insecurity. To all these if we add the imbalances between the member states regarding the participation at NATO's budget, the emergence of states that do not comply with the treaties of non-proliferation of nuclear arms, the most obvious example here is Iran that despite all sanctions and external pressures continue to develop its nuclear program, we reach to the conclusion that depending on how NATO will be able to find the answers needed to solve these problems depends both its future as well as the Euro-Atlantic security.

The generation of resources also remains a problem faced by the Alliance in the current economic crisis. To be able to spend less and more efficiently, in terms of generating

capabilities, in order to achieve the goals established within the new Strategic Concept, NATO launched at the Chicago Summit, held May, 20-21, 2012, Smart Defence initiative[1].

This initiative comes in support of the member states by providing alternative solutions to their problems that are mainly due to the difficult financial situation.

Smart Defence initiative is guided by the following principles: greater flexibility of the alliance; better interoperability for member states when they are put in a position to carry out joint multinational operations; establish clearer priorities, in line with the national defence strategy and by doing an concrete assessment of the threats that could threaten any member state; developing a set of common projects that will take place in three stages, depending on their need to the Alliance, their importance, as well as how these projects will find a lead nation.

Each NATO member will invest in defence projects which are a real need to the Alliance, and not in generating its own defence capabilities. Our opinion is that, through this concept we can achieve the optimization of the capabilities that are needed to accomplish the strategic objectives[2].

The actual purpose of this initiative is to generate the required capabilities for Alliance, to maintain in operable condition the existing ones and to train forces to arrive at a best possible training level. It should be noted that the main role in the development of the Smart Defence initiative is held by member states as, only through their active participation in various projects, they can achieve the proposed goals, because this initiative is created by nations, for them and through them. Also this initiative tries to strengthen the relationship between NATO and the EU.

The development of this initiative will provide for the European allies a set of capabilities that are needed to accomplish the proposed objectives. It has been observed in various occasions that the EU needs to develop its own set of capabilities. In this way the Union will not have to use NATO capabilities under *Berlin Plus*[3] agreements. EU attempts to create these capabilities by Pooling and Sharing initiative. In this context, NATO must work closely with the EU to ensure that the two initiatives complement each other, thereby avoiding any engagement of both in the same projects. So between the two organizations it must be a continuous communication and transparency regarding their objectives and their projects.

National commitment is a primary factor in the development of this initiative. Despite its multinational nature without the support of each ally, and without their active involvement the development of the initiative would not be possible[4].

We can define the elements of Smart Defence initiative as follows[5]:

- prioritization: refers to the fact that the allies need to align their priorities in terms of capabilities to NATO standards, going over the national thinking. Taking everything into account, we will see that a prioritization of spending, according to the requirements of the Alliance, will lead to a more effective national budgetary spending and create a set of capabilities that normally would not have been possible without the initiative;

---

[1] See Lt.col. Dumitru Cristinel COLIBABA, research paper Nr.1, "Operations of coalition- The success of future conflict" Publisher National Defense University "Carol I", Bucharest, 2012 p.46.

[2] See http://www.nato.int/cps/en/natohq/topics_84268.htm?, accesed on 08.09.2014.

[3] The arrangements "Berlin Plus" were completed in the spring of 2003 and refers to the EU access to NATO operational planning capabilities; the EU's access to NATO's collective military means; European command options for EU operations carried out with recourse to NATO resources (DSACHEUR operational commander acting and SHAPE on the operational command).

[4] See Teodor FRUNZETI, "The concept of "Smart Defense" in the context of an efficient defense planning", in *Journal of Defence Resources Management*, Vol. 3, Issue 2(5)/ 2012, Brasov-Romania, p. 9.

[5] See Constantin MINCU, NATO "SMART DEFENCE" between the theoretical concept and reality", in *Journal of Military Sciences*, published by the Department of Military Science of Scientists in Romania, p. 12.

– specialization: with budgets under pressure due to the economic crisis, some NATO countries (including here Romania) have abandoned or postponed some capabilities, without regard for the needs of those capabilities in the future. This has led to increased spending for other allies, particularly for the USA, which recently gave clear signals that it is no longer willing to make this effort and asked the allies to increase efforts regarding NATO budget. Defence budget cuts, uncoordinated, which occurred after the beginning of the economic crisis, seriously damaged the Alliance ability to face the multiple challenges of the 21st century. NATO, through Smart Defence initiative is prepared to encourage specialization on projects, because each ally has its own national strong points, while maintaining national sovereignty for their final decision;

- cooperation: by working together, the allies can have access to capabilities that they could not afford on an individual basis. Cooperation can take various forms such as a small group of nations, led by a lead-nation, or strategic sharing between those who are close in terms of geography, culture or common equipment.

The pragmatic initiative of smart defence has multiple purposes[6]:

• to boost European pooling & sharing program, which based on defence cooperation;

• to decrease the spending on defence capabilities for the states involved, while ensuring the necessary capabilities;

• to support the technological research and the programs regarding the development in this area;

• create a competitive market for defence equipment;

• to create a common market as regards the purchase of weapons and materials of this nature.

All these goals are designed to create a set of capabilities required by NATO, so that the Alliance can achieve its main objective, which is to maintain its capacity of guaranteeing Euro-Atlantic security.

Nations continue to discuss promising areas for multinational cooperation such as logistic cooperation, collaborative training opportunities, and protection of forces. Smart Defence projects are funded by participating nations[7].

We will try further to work on a brief summary of the projects developed in the Smart Defence initiative and to detail the development of the most important ones. Such ongoing projects of Smart Defence initiative are in number 26 as follows[8]: NATO Universal Armaments Interface; Remotely controlled robots for clearing roadside bombs; Pooling Maritime Patrol Aircraft; Multinational Aviation Training Centre; Pooling & Sharing Multinational Medical Treatment Facilities; Multinational Logistics Partnership for Fuel Handling; Deployable Contract Specialist Group; Immersive Training Environments; Computer Information Services (CIS) E-Learning Training Centres Network; Individual Training and Education Programmes; Multinational Joint Headquarters Ulm; Female Leaders in Security and Defence; Joint Logistics Support Group (JLSG HQ); Pooling of Deployable Air Activation Modules (DAAM); Theatre Opening Capability; Multinational Military Flight Crew Training; Counter IED – Biometric. To all these, there could be also added the establishment of a Multinational Geospatial Support Group (GSG); Multinational Cyber Defence Capability Development (MNCD2); Harbour Protection; Pooling CBRN Capabilities, the development of Personnel Reserve Capabilities; Alliance Defence Analysis

[6] See Filofteia REPEZ, "Smart Defence A new approach to collective defense within NATO", in *Romanian Military Thinking*, no. 1/ 2013, p. 81.

[7] http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2014_06/20140602_140602-Media-Backgrounder_Multinational-Projects_en.pdf accessed on 09.09.2014.

[8] http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2014_06/20140602_140602-Media-Backgrounder_Multinational-Projects_en.pdf accessed on 09.09.2014.

and Planning for Transformation (ADAPT); Defensive Aids Suite (DAS); Integrating Explosives Safety and Munitions Risk Management (ESMRM); Malware Information Sharing Platform (MISP).

NATO Universal Armaments Interface. This project will enable fighter jets to use munitions from various sources and nations. It will facilitate the flexible use of available munitions across the Alliance and promote multinational cooperation. The air operation over Libya has demonstrated the importance of such a project. It is very important that the Alliance is trying to learn from past lessons and to develop such projects, in the future to be able to face all challenges.

Remotely controlled robots for clearing roadside bombs. From the lessons learned in Afghanistan, the Alliance is looking to develop a program that would not need to risk the lives of soldiers on mission and instead to develop a program based on robots that can defuse IED placed on the roadside.

Pooling Maritime Patrol Aircraft. Through this program NATO attempts to create a capability, both for countries participate in it, as well as for other member countries at their. The Alliance will develop such a program that will bring together more jets to patrol the territorial waters of member countries.

Multinational Aviation Training Centre. This program is also based on experience gained in Afghanistan and involves the training of helicopter pilots for various missions that will follow, and the training of crews that will be at the ground.

We must mention that the initiative has completed 6 projects such as: Multinational Logistics Partnership – Helicopter Maintenance; Dismantling, Demilitarization and Disposal of Military Equipment (D3); Centers of Excellence as Hubs of Education and Training; Multinational Logistics Partnership - Mine Resistant Ambush Vehicle (MRAP) maintenance; Multinational Cooperation on Munitions (Munitions Life-Cycle Management); Weapons Systems – Managing spare parts[9]. This first projects, developed under the initiative, enjoyed a great success and they can be accessed by all members of the Alliance. They have made a major contribution into creating a much needed set of capabilities for future operations, and also for ongoing operations at this moment.

Multinational cooperation must further be carried out in order to continue other projects such as: NATO's Missile Defence capability, through which NATO will have a full range of capabilities to defend against long-range missiles. Several European countries have shown the interest regarding the participation in this project, but the main contribution will be made by the United States; Alliance Ground Surveillance Programme (AGS) in which 15 allied countries have developed an air surveillance system that from which will benefit the entire Alliance and who is supported in financial terms by all members, and those who will not be able to contribute financially will have to provide to NATO their national capabilities in order to develop this program; NATO Air Policing –in this project NATO offers its own fighter jets to the performance of air police missions of the allies, this means reducing costs in some states in the execution of this mission and even coming to meet some states that are facing with some problems because of the need to change their military air fleet; Joint Intelligence, Surveillance and Reconnaissance (JISR).

According to the official response given by the Ministry of Defence in regarding the Romania's participation in projects developed within the Smart Defence initiative, our country has expressed its intention to participate in a total of 40 projects for the development and use of NATO capabilities from a total of 150 projects, as follows:[10]:

[9] http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2014_06/20140602_140602-Media-Backgrounder_Multinational-Projects_en.pdf accessed on 11.09.2014.
[10] http://www.cdep.ro/interpel/2013/r853A.pdf accessed on 10.09.2014.

- *Pillar I* - 29 projects recommended that have a lead nation, and can be implemented in the first phase, 15 of which Romania is declaring her intention to participate;
- *Pillar II* - 54 possible projects in which the nations manifested a moderate desire for participation and it was not identified a lead nation.. Of this total of 54 our country has expressed its intention to participate in a total of 18 (two of them as a state observer);
- *Pillar III* - 67 project proposals received from defence industry and the nation, which can not currently be developed due to lack of financial resources and the lack of interest shown by the members of the Alliance.

Smart Defence is for our country a solution to problems concerning the gap of much needed capabilities to carry out a military operation. Also the country's participation in multinational joint operations is put lately in balance by other nations because of the lack of these capabilities that could allow us to successfully carry out a military operation.

The Ministry of National Defence carries out various programs in close collaboration with representatives of the defence industry, in order to achieve common projects and to revitalize the sector. One such project was conducted during the meeting *Info Day,* for the development of some plans regarding Romanian participation in projects under the first pillar of the initiative.

According to the Minister of Defence, Romania has gained significant experience in the field, our country is currently an active member in projects such as: the NATO Airborne Early Warning Capability (NATO Airborne Early Warning - NAEW), the Alliance Ground Surveillance capability (Alliance Ground Surveillance - AGS) and the strategic airlift capability (Strategic Airlift capability - SAC)[11].

Supporting the idea that in order to have a Euro-Atlantic sustainable defence sector, technologically advanced and globally competitive, Foreign Minister Titus Corlatean, had declared that "this desire can only be achieved through the convergence and the cohesion of the policies in the field of the allies, and that ambitious goal of transforming NATO defence requires a common approach to defence industry policy grounds"[12]. Just in this section Romania is deficient. Arms industry in our country is in a constant decline, due to wrong policies regarding the investment and the modernization plans of the sector.

Another important project in which Romania takes part is the acquisition of multirole aircraft, in consortium with Bulgaria and Croatia. Any costs that will arise from the purchase of these aircraft will then be divided among the three states and also costs of maintenance and pilot training. Our country has shown its willingness to create a Smart Defence initiative, in collaboration with other interested states, a cyber defence program with the help of Romanian hackers[13].

In the Declaration of the recent ended Summit, that took place in Wales, NATO Heads of State and Government from the member states have agreed that within a decade to allocate a percentage of at least 2% of GDP on defence, as seen through international agreed obligations when they became members of the Alliance. This may revitalize arms industry and investment in the field of defence.

[11] http://jurnalul.ro/stiri/politica/dusa-romania-intentioneaza-sa-participe-la-proiecte-dezvoltate-sub-egida-smart-defence-666959.html accessed on 11.09.2014.
[12] http://www.mae.ro/node/16355 accesed on 12.09.2014.
[13] See Filofteia REPEZ, "Smart Defence A new approach to collective defense within NATO", in *Romanian Military Thinking*, no. 1/2013, p. 83.

Conclusions

We have to understand the idea that through this initiative every member of this Alliance can create a set of capabilities, that are so much needed, in an efficient and economic way, and their sharing will transform NATO into a stronger and more flexible organization.

Although at the beginning some members were sceptical about the success of this initiative, during its development more and more countries have shown interest and participated actively in projects developed within it. Its chances of success are even more as the economic crisis makes it difficult to achieve such a goal by a single state. The governmental environment should work closely with the private sector in order to develop a set of new capabilities in order to face the new threats.

For Romania, this initiative represents a unique opportunity to develop a much needed set of capabilities, in the current context of the decline of the defence industry and the economic crisis that reduced budgets, and therefore investments in this area.

We firmly urge that is needed a standardization for procurement of the defence related materials and that so acquisitions would be made in a transparent manner. The emergence of such a standard will give to all states the possibility to know and participate in auctions and thus this we will add value to all acquisitions.

Our country can focus on those sectors of the defence industry that are still functional and in which we have a tradition, in order to revitalize them and to be able to compete with various countries in the export of arms, or acquisition of such materials on the national territory.

Further participation in projects in the Smart Defence initiative of our country is, in our opinion, impetuously needed in order to deal with all threats that are to come, and that our state may become a puncture of the reference point regarding the security of the allies in the Black Sea area and the Balkans.

Acknowledgement:

This work was possible with the financial support of the Sectoral Operational Programme for Human Resources Development 2007-2013, co-financed by the European Social Fund, under the project number POSDRU/159/1.5/S/138822 with the title ***"Transnational network of integrated management of intelligent doctoral and postdoctoral research in the fields of Military Science, Security and Intelligence, Public order and National Security – Continuous formation programme for elite researchers - "SmartSPODAS"."***

BIBLIOGRAPHY:

1. COLIBABA, Dumitru Cristinel, Research Paper No.1, "Operations of coalition- The success of future conflict", "Carol I" National Defence University, Bucharest, 2012.
2. FRUNZETI, Teodor, "The concept of "smart defence" in the context of an efficient defence planning", in *Journal of Defence Resources Management*, Vol. 3, Issue 2(5)/ 2012.
3. MINCU, Constantin NATO, "Smart Defence" between the theoretical concept and reality", in *Journal of Military Sciences*, published by the Department of Military Science of Scientists in Romania.

4. REPEZ, Filofteia, “Smart Defence A new approach to collective defence within NATO”, in *Romanian Military Thinking Magazine*, No.1/2013.
5. NATO official web page, www.nato.int.
6. Romanian Ministry of Foreign Affairs official web page, www.mae.ro.
7. Romanian Government official web page, www.gov.ro.
8. Romanian Ministry of National Defence official web page, www.mapn.ro.
9. European Union’s official web page, www.europa.eu.
10. Official web page of the Chamber of Deputies of the Romanian Parliament, www.cdep.ro.

DIMENSIONS OF THE ASSESSMENT ACTIVITIES FROM SPECIFIC INSTITUTIONS UNDER NATIONAL DEFENCE SYSTEM

Dorin-Marinel EPARU
Colonel, Assistant Professor, PhD. Security and Defence Faculty,
"Carol I" National Defence University, Bucharest, Romania.

Abstract: *Assessment theory and practice holds a variety of approaches and evaluative understanding of joint actions.*

In the specific institutions of the national defence system - the evaluation is a function of management with foresight, judgment, planning, organization, coordination and control activities. Of course, the horizon, goals and evaluation differs depending on the level at this is made.

Summarizing, we believe that this assessment relates to the activity where that information is collected, processed and interpreted. The interpretation also refers to the condition and operation of the system and the results processed by the institution, leading to appreciation of their activity on specific criteria and influencing the evolution of the system.

Keywords*:* evaluation, management, national defence system.

Theory and practices of educational assessment records a variety of approaches and evaluative understanding of joint actions. They are nuances in terms of understanding the nature of this process, which is the subject of evaluative activities, the functions they perform, as well as manners of achievement.

Many times, the assessment of education's outcomes is diminished to actions as: to check, to research, or to note. The same, the assessment action is understood as "to appreciate" (good, poor, brave, timid military) and "to classify" (the best, the last in the platoon, he/she is part of the middle category etc.). Also, many practitioners (trainers, instructors) limit the object of evaluative actions to the reached goals, ignoring numerous components of training activity which are the object of assessment: educational processes, teaching personnel training, structures to educate etc.

1. The analysis of the assessment activity

To give a complete answer to the question "*What does mean the assessment?*", it should be said that assessment is more than a job or a technique, but a "complex action, a set of mental, acting and intellectual operations, attitudes, and effects"[1] that it is assumed that states: contents and goals to be assessed; what purpose and what perspective is evaluated (the perspective of evaluated decision); when considering the assessment (early training, during the training, at the end of balance); how to assess; based on which criteria is assessed and how data are processed and information are valued.

Trying a "scan" of assessment, Alain Kerlan[2] believes that the evaluation involves a systematic and surgery design starting from several key questions:

• Why to do it? (Which highlights the functions of assessment);

[1] Vasile GRAD, *Cercetare operaţională în domeniul militar,* Sylvi Publishing House, Bucharest, 2000, p. 72.
[2] Alain KERLAN, *Les didactiques entre instruction et instrumentation,* Revue du CRE, Universite de Saint–Etienne, 2000, p 24.

• In relation to what is do it? ("References" - criteria of evaluation);
• For who is do it? (Recipients of evaluation);
• What? (Which is evaluated);
• How? (Tools and procedures used for assessment).

From the perspective of understanding the nature of this process and how to achieve it, there is a diversity of viewpoints in the assessment theory. It is reflected in the variety of definitions of evaluative act.

Naturally it is not possible to fully present them, so we bring to the attention a few *defining terminology and practical implications*. By way of example, we retain the most often used.

Thus, B. Bloom understands evaluation as "*formulation, for a determinant purpose, of judgments on the value of certain ideas, papers, statements, methods, materials, etc.*"[3] So, the assessment involves the use of criteria to settle how certain actions, processes are efficient, economical or satisfactory.

It is also known that value judgments may be quantitative and/or qualitative. We must remember, as basic elements that: evaluation *requires* a value judgment on the state of the assessed phenomenon; it *requires* both quantification (measurement) and the appreciation of the phenomenon; value judgments *involve* the use of criteria, especially since everything is done "in a specific purpose".

Also, A. Bonboir defines evaluation - like B. Bloom - as implying "*a value judgment based on specific criteria; it can have a numeric result (note) or grade (subject classification into a class, setting known content elements etc.)*" [4].

Assessment is similarly understood by J.P. Caverni and G. Noizet defining it as "an action by which, on an object, event, person is made a judgment in terms of criteria"[5]. Such a judgment usually becomes expression in qualitative assessments, verbal comment or numerical forms.

Other definitions consider evaluation as a process consisting of "*gathering information*" [6] in a systematic way, on a system.

These definitions emphasize distinctive notes of evaluative act. Most relate to the same component actions and operations - gathering information about the condition and operation of a system, its assessment, reporting to a purpose and so on, but still remain incomplete.

Looking at these definitions of assessment is noted that:

- evaluation is a process (not a product), so a phased activity held in time;
- It is not about scoring (which is a numerical expression of assessing performance), but also covers more complex areas and issues (including curricula and training system as a whole);
- assessment involves a series of measures, comparisons, appreciations (i.e. value judgments), on which certain decisions may be taken designed to optimize the activity of the areas under evaluation;
- Assessment itself does not mean anything other than measuring staff/ structures' training deficit from predicted performance standards.

By the same analyzed set, we found that, relative to its subject, the *assessment* is done both *at the system level* and *at the training process* level.

---

[3] Irina – Ioana JUNC, *www.iTeach.ro*, *Centrul pentru Inovare în Educaţie*, accessed on 30.09 2014.
[4] A. BONBOIR, *Definiţiile evaluării*, www.pdf-repo.com, accessed on 02.10 2014.
[5] J.P. CAVERNI şi G. NOIZET, *Definiţiile evaluării,* ro.scrib.com/doc/167310752, accessed on 02.10 2014.
[6] P. F. DRUCKER, *Management Challenges for the 21st Century*, Butterworth-Heinemann Elsevier, Oxford, 2007, p. 83.

System's assessment is, as the name implies, the rigorous assessment of the extent to which that system operates normally, according to the rules of law, and intentions of leaders at various levels, i.e. those who conceive and design policy in that field. "*By system's assessment are considered both the results of this policy and whether the policy itself was adequate for the ideal educational requirements and actual requirements of the society in the short, medium and long term*"[7]. Once developed, this policy sets out what will actually take in some stage of system development, in training and education plan in order to achieve educational ideal.

System's assessment is (if we can speak so) analytic-synthetic, as does a comprehensive analysis of the operations and results of system/subsystem, but insisting also on those elements that are "strengths" and "weak points" coming of it, to make relevant decisions to liquidate/decrease failure and to encourage initiatives, innovations that generate superior performance. *Process' assessment* aims the whole educational process or certain elements of it.

In both cases (the assessment of system and of process) are targeted areas and issues such as: outcomes, curriculum, organization forms, educational methodology, staff training and development (teaching, support and administrative), logistics, financing, management and like. Obviously, at the level of the educational process, the emphasis is on quality of training and especially on the acts of teaching and learning that influence and determine the ultimate performance of the personnel within specific institutions of the national defence system. Of course, the horizon, goals and evaluation issues differ, depending on the level at which is done. From this point of view, there are the following levels:

- *at the system level,* assessment is made in particular to make correct decisions of educational policy, as well as to improve the curriculum, methods of training of staff, management system, research profile etc.;

- *at the level of the process of preparation,* assessment provides information to improve the school network, the optimal use of human and material resources, coordinating institutions of subsystem, etc. improve the management of educational institutions, according to specific tasks;

- at the institution's level, the assessment as a function of management, aims "all that moves" in that institution, but especially the education and performance of employees because a "commander", good manager, takes care of his/her institution's "prestige", and the system requests it to prepare students especially in light of the results, the fame that has created in the system, but also at regional/national level.

Finally, *each instructor's assessment* is the most systematic and timely and (due to direct daily contact with staff training) the most accurate, although instructors are not always willing to provide partial results as they appear during the course of training. Their reserve is justified by pedagogical reasons as positive motivation is more beneficial than negative when educating students. Only at this level, assessment exercises formative, progress function, and the underpinning diagnosis approved by the instructor optimizes the teaching and learning documents.

Training institution and structures remain, ultimately, the "hottest" areas of staff performance assessment. Information obtained through evaluation at these levels, underlay continuous action to improve the educational process harmonizing (when driving jurisdiction) goals and contents, forms and instructional strategies, interests and aspirations, material and human resources.

In an attempt to integrate different points of view, to make compatible different definitions, we need to reveal the main dimensions of evaluative act of the institutions of the

[7] Zlate MIELU, *Leadership şi management*, Polirom Publishing House, Bucharest, 2004, p. 138.

national defence system. With their knowledge, properly evaluative approaches produce a genuine "energizing effect" of the subjects, a strong infusion of engagement towards improving the system to which they belong.

2. Formative, normative and systemic dimensions of the assessment management of the national defence system institutions

Essence complexity of management process requires a detailed analysis of its main key notes (size), which explains mechanism, process, actions designed and built, selected contents, chosen strategies, criteria and modalities of assessment, stakeholder relationship, structuring in time and even system optimization.

2.1 Formative dimension of assessment activity management

Formative dimension of assessment activity management still being accepted on this position requires:

- Facts recognition in the content, teaching strategies to "overthrow" the traditional triad of goals: knowledge - skills and abilities - intellectual attitudes and skills in spiritual attitudes and capacities - skills and habits - knowledge (concepts and methodologies);
- Bringing to the fore the qualitative aspect of training cognitive processes to solve various situations involved in the assessment of training;
- Training of intellectual qualities to find concrete expression in the formulation, specification, operational objectives for the assessment activity, prior for training;
- Use of "multipurpose formability" to highlight the requirements of the future that will need skills, abilities, operational schemes, acting and attitudinal structures, especially capacities: general operators that establish relationships and causes necessary for continuous training, to establish relationships of communication, adaptation to changing environments and business profiles, perfecting, etc.;
- Changing attitudes towards information as concerns the following aspects: volume reduction, removal of obsolete and detail knowledge, essentialization, increasing the applicative and operational value.

That means in teaching – training activity, information becomes means with which knowledge, understanding etc. is shared and the student is trained in carrying multiples tasks, to the detriment of their transmission dominance in the traditional sense by the instructor;

- Training by active learning also changes the acting sense of the assessment and follow-up the independent intellectual work style, of motivation for continuous training;
- In terms of increased safety, formative assessment management will be real in future social activity is useful for training curriculum, and try to remember to order the possible intellectual approaches involved, then: the acquisition of new information and their treatment, finding relationship to the environment, development communication, translation of a message from one code to another, adapting to new situations, using different models, problem solving, creativity assertion, making assessment criteria, generalizations and transfers even build capacity to explain, to demonstrate, to provide, to act rationally decide, to devise a strategy or action plan, organize.

Difficulty of these formative dimensions fulfilment is obvious but basically educational reform will have to take because there is needed to be created the conditions of its application.

Some of these conditions: changing attitudes over learning objectives; appropriate selection of the content, which allows the various operations - task information; call for the use of theories, models, active learning modes; teaching methods, ways and forms of organization of students activities to promote real, differentiated self-employment learning; changing conception of training: the dominant transmission conditions to become

organization of condition of education, coordination, stimulation of training, direct operation of information.

Explicit awareness of staff trained on the objectives, their possibilities, techniques and modes of instruction, assessment criteria and forms is still a goal to be implemented.

2.2 The normative dimension

The specialty literature has not explicitly approaches of normative as a feature of the assessment process management, but includes it among the components of the instructive-educational action by association with the category of assessment "principle".

With due and balanced theoretical, practical and actionable assessment process, so necessary when we refer to the institutions of the national defence system, we find that we must dissociate, see right the relationship among time and principle.

Traditionally, the "principle" term is associated with legit character of training, through a generalization of the practice, from which depends on the organization and coordination of overall orientation and adjustment. The principles provide general orientation of the assessment process as legitimate but actual praxiologic coordination of the various actions, situations of application, and who does it.

Seeking the answer, we find that the assessment process, in the achievement of its intimate, practical, practice in order to achieve the effectiveness of its actions requires a "reassessment" of the place and role of norms and rules of application.

According to dictionaries, and managerial direction, the rule indicates one or more binding rules in carrying out the action, the minimum conditions to be met and then considers the success of the action, optimal prescriptive of deployment sentences, practical information, specific on obligations, prohibitions, permissions action, and respected algorithms. Then normative action management of assessment process is both the provisioning of those requirements, rules, requirements that have been effective time of specific actions, and use each of them in logical sense and law-like, the assessor / assessed field respects a powered algorithms body, a set of evaluation criteria, and can prove their craftsmanship in combining art, after situation.

In common language normatively is frequently played using expressions: *"should / should not" ... "it is allowed / not allowed" ... "can / can not" ..., "if that, realize ... then ..., that is required to be" ..., "learn to repeat N times" ..., "apply the following rules, the following steps, stages"..., "follow the following pattern ... it is fair to" ...* etc. Such concrete prescriptions we abundantly find in the presentation of assessment process components for the scientific grounding, by generalization as well as by practical applicative opening.

Due to the normative feature of assessment action strongly felt in the practice, *many experts*[8] call "assessment" to be technological, practical/applied, methodological science. Current studies addressing such normative dimension of management process assessment reveal some useful aspects for an effective approach to managerial action:

- *Assessment rules* must be *consistent with the educational norms*, by nature of domain, and can be - organizational, procedural, communicative (relationship assessor-rated), mandatory or permissive, general or particular, guidance for future action, inhibitors of a particular behaviour;

- *Each component element of the process/action* assessment *implies a prescriptive element;*

- *Rules of assessment process* presented in the theoretical, explanatory and praxiologic approach are more or less widely used and respected. "As much the assessor and the assessed

[8] *Evaluare.ppt-MTS-SM*, www.mts-sm.wikispaces.com, accessed on 03.10.2014.

know the scientific normatively aspect of progressive assessment process, as much it can manifest creativity, explore and optimize their activity"[9].

Therefore, the rules are criteria for assessing the competence of educational, professional maturity degree of affirmation of professional skills.

2.3 The systemic dimension of the assessment process management

Because literature used to explain the assessment action does not specify explicit but rarely the relation to this "dimension" of the evaluation process as a system, in practice there are many unintended consequences, often leading to formalism: low baseline analysis for choosing the best strategies, poor learning opportunities for networking between the components for making the choice of methodological and organizational assessment situations etc.

Other aspects of effective assessment also draws us attention the use of systemic interpretation of assessment activity management: notification and real solving of effects highlighted by reverse connection, mastery and application of self-assessment and objective criteria for each operation or activity, knowledge and application of optimal assessment theory, training and rapid processing skills accumulation of the information coming from the outside of the system elements and prevention of system's dynamics (even in a simple assessment situation) relative to the level of their elements, risk awareness and how to avoid , providing changes that may occur in components etc.

By accepting and using this dimension of assessment activity management, the practitioner gains an important methodological tool to optimize its action, at any level, because he/she can learn more about the system, elements and interrelationships, can continuously analyze its dynamics, can prevent and relieve functionality (in relation to the goals) and the efficient undergoing (relative to the determination of actions, steps, procedures, factors).

Both in theory and in practice, the assessment work can be seen as a cyclical process with particular sequences (points, stages, links, etc.) taken in a certain sense, consisting of interconnected activities, performed to achieve a certain purpose. Regardless of the terminology used to define moments of assessment work management process, it has the following structure:

- Analysis of the managed system, with its three sequences - *postfactum* analysis (referring to a more or less close past);
- Diagnosing the *status quo*; forecasting analysis (embodied in identifying possible trends of development of the evaluated system);
- Specifying the desired and also possible goals; determining the path of action to achieve the goals; detailed objectives and subsystems distribution, identification and distribution of resources, prioritization; system organization to achieve the goals of the evaluation (design, development and improvement of structures, establish responsibilities, selection and training of personnel, etc.);
- Transmitting orders, motivating, training and managing the participating subsystems to accomplish the mission; harmonization efforts, removing differences, changing rhythms and spatial relationships;
- Monitoring, itself assessment and eventual correction to the accomplishment of the objectives.

Design of the assessment activity process of management as a cycle of analysis, decisions and actions should not be rigidly interpreted containing identical issues in all cases and not necessarily in the sequence of steps *a priori* established and designed.

---

[9] Cf. Elena JOIŢA, *Eficienţa instruirii, Fundamente pentru o didactică praxiologică*, Didactică şi Pedagogică R.A. Publishing House, Bucharest, 2002, p. 43.

"*The process should not be a barrier to creative expression*" [10].

To avoid distortions in one way or another (i.e. by over or undervaluation), control structures of the institutions and other specialized bodies within the national defence system are also doing assessments and obtained information compare with those of internal assessors, and therefore they can adopt such measures accordingly. Here, then, assessment can not be separated from the context of the system and the process of preparation.

Conclusions

Assessment activity in the framework of specific institutions of the national defence system is an activity of *a special type of knowledge*, presenting some distinctive notes. It does not aim to produce new knowledge, to validate assumptions, to build or to systematize theoretical constructions. The dominant function of the assessment is not to explain a phenomenon, although in some cases, at least indirectly, such a function is present. Evaluative act should aim to improve the state of the evaluated phenomena, being made towards making decisions of this nature, which underlies. The assessment is such fulfilled for a distinct usually immediate purpose, as follows:

a) *Assessment is an act of (specific) knowledge* of some phenomena in terms of their characteristics, condition and functionality of a system, the results of activities. Therefore, "*the object of the assessment can be a phenomenon, a person, an activity or its outcomes, an institution, or the overall system, etc.*" [11]

As an act of knowledge, the assessment presents here some common notes with the knowledge process in its epistemological sense. Both are processes of knowledge, undertaken for defined goals, using appropriate methodologies and tools and involve operations of data processing and interpretation.

b) *Knowledge obtained in the context of the assessment is done to achieve a goal* and derives from the need and therefore the intention to influence the situation, the system, the activity being assessed, in order to adjust them, so to create the prerequisites for improving their condition and functionality. Referring to evaluation in education, Torrance believes that *an "authentic assessment" is designed to improve teaching and learning practice*.

This feature highlights the lack of opportunity and inconsistent, proactive administrative interventions, aiming to improve an activity without a more objective assessment of its condition. In the case of the social and human systems, the utility of assessment considerably improves by the impact it exerts on the subjects involved in the evaluated system. Evaluative approaches generate to the subjects of the assessed system the so-called "conscience plug", with favourable effects on their activity and behaviour and even on the organizational climate.

Under the circumstances of their achievement, the evaluative initiatives produce a veritable „effect of subjects' energizing", an infusion of stronger employment in order to improve their system.

c) In connection with the function of improving the phenomenon under measurement, *the assessment involves a process of data collection* necessary to support decisions to be taken in order to improve considered activity and results. Data collection is an important and complex approach of the assessment, by which depends in large measure, the effectiveness of evaluative act. In this sense, assessment efforts are aimed to provide useful information to decision-makers responsible for carrying out training. Located within the evaluated system or

[10] Aurel Nour, *Fundamentele conducerii militare*, PublishingHouseConsult, Bucharest, 1998, p. 24.
[11] A. Novak, *Metode Statistice în Pedagogie*, PublishingHouseDidactică şi Pedagogică, Bucharest, 1977, pp. 60-67.

to the level of outside authorities, the assessors are mandating the assessment, but also the main recipients of valuations.

d) Another component of the assessment process is *the management of obtained information.* Evaluative process involves actions (sequence) of processing and interpretation of the collected data, in which many operations are performed on obtained information by assigning meaning to those information, transforming them through their translation by a "language to another" when necessary, conduct comparisons, putting in relation to expected results (goals), formulation of evaluative function statements (acceptable / unacceptable, marks etc.).

e) *The assessment involves appreciations of the evaluated situations related to various criteria* (social, cultural, performance, feasibility, etc.). We know that the assessment is a valued act involving an axiological attitude. It requires issuing of value judgments on the assessed phenomena by comparing the obtained data to a system of values. The existence of normative perspective, embodied in the criteria the obtained data are reported to, should be a feature for the evaluation carried out within specific institutions of the national defence system.

f) *Evaluative actions require methodological approaches and attitudes* embodied in: completion of defined stages; recording the data in a manner that ensures accuracy and conservation, using various tools (charts, reports, documents, boxes, etc.); assessment approach concern to ensure quality and validity, relevance, fidelity; identify relationships between obtained data and between them and various features of the system under assessment, especially when you can not apply their strict evaluation rules and are done recourses to global assessment ("Best Judgement"); use of specific forms, strategies, methods and techniques.

g) *The assessment produces an anticipatory effect,* making - among other things - also a predictive function on the evolution of evaluated system and its results (wash forward). Note that, in some cases, may occur retroactive effects (wash back) such as, for example, need to complete gaps, correct errors in all subjects of the acquired knowledge.

Summarizing these common characteristics, we believe that broad assessment relates to the activity in which framework information is collected, processed and interpreted on the condition and operation of the system, and the results you get, and this activity leads to their activity assessment grounded on criteria that influences the future evolution of the system.

Acknowledgement:

This paper has been financially supported within the project entitled ***"Horizon 2020 - Doctoral and Postdoctoral Studies: Promoting the National Interest through Excellence, Competitiveness and Responsibility in the Field of Romanian Fundamental and Applied Scientific Research",*** contract number POSDRU/159/1.5/S/140106. This project is co-financed by European Social Fund through Sectoral Operational Programme for Human Resources Development 2007-2013. **Investing in people!**

SELECTIVE BIBLIOGRAPHY:

1. BURDUŞ E., *Management,* Economică Publishing House, Bucharest 2005.
2. CERGHIT I., *Sisteme de instruire alternative şi complementare, structuri, stil şi strategii,* Aramis Publishing House, 2002.
3. CRISTEA S., *Teorii al învăţării – Modele de instruire,* Didactică şi Pedagogică Publishing House, Bucharest, 2005.

4. EPARU M.D., *Sistem e-learning în învăţământul militar românesc,* E-Learning and Educational Software, Scientific Communication Session, Challenges against security and strategy in the XXI century, Bucharest, April 2005.
5. GHICA Dan, CHEŢE Emil, *Transformarea militară – coordonate instructiv – educative,* CTEA Publishing House, Bucharest, 2010.
6. GRAD Vasile, *Cercetare operaţională în domeniul militar,* Publishing HouseSylvi, Bucharest, 2000;
7. JOHN GARSTKA, *The transformation challenge*, in „NATO Review", no. 1, 2005;
8. Kerlan Alain, *Les didactiques entre instruction et instrumentation,* Revue du CRE, Universite de Saint–Etienne, 2000;
9. NICOLESCU O., *Fundamentele managementului organizatiei,* PublishingHouseTribuna Economică, Bucharest, 2001;
10. NOEL TICHÝ, *Liderul sau arta de a conduce,* PublishingHouseTeora, Bucharest, 2000;
11. NOVAC J. D., *A Theory of education, Ilinois,* Cornell University Press, 1977;
12. RADU I.T., *Evaluarea în procesul didactic,* PublishingHouseDidactică şi Pedagogică, Bucharest, 2004;
13. ZLATE M., *Leadership şi management,* PublishingHousePolirom, Bucharest, 2004.

Webgraphy:

* * * http://www.mapn.ro/strategiasecuritate
* * * http://www.biblioteca-digitala.ase.ro
* * * http://www.technoscience.net/?onglet=glossaire&definition,
* * * http://www.nato.int/docu/review/2010/issue1/special.html.
* * * www.actrus.ro
* * * http://dexonline.ro

ACADEMIA – A STRATEGIC RESOURCE FOR THE INTELLIGENCE COMMUNITY

Oana SANDU
PhD candidate, "Mihai Viteazul" National Intelligence Academy.
E-mail address: oanasprincenatu@yahoo.com

Abstract: *The relationship between Intelligence Services and Academia has been increasingly debated in the last decade, although it has existed in different forms, for over half a century. The security environment, be it national or global, has suffered tremendous changes after the Cold War, which have forced intelligence to reshape itself, as its mission continuously encompasses new dimensions (terrorism, health, environment, cyberspace, and so on). Intelligence communities are no longer puzzle-solvers but knowledge seekers that try to make sense of the complexities that are arising rapidly. In order to answer the new requests of their beneficiaries, intelligence agencies need to reach out to other knowledge seekers, such as scholars. The current paper tries to explain why a closer relationship needs to be established between the two communities, emphasizing not only its benefits, but also its limits. Moreover, we will be looking at some outreach policies that have been implemented thus far in different countries and we will also analyze the Romanian case.*

Keywords: *Academic outreach, Civilian Intelligence Reserves, Intelligence Communities, Knowledge Society, intelligence culture.*

At least two historical landmarks have had an important impact on intelligence as activity, product and structure. The first one is the end of the Cold War, with all its consequences on the international order, that have implicitly changed the scope and targets of the intelligence agencies. At that time, there were many voices, especially in the United States, that argued for a restructuring of intelligence agencies, in terms of reducing personnel and resources, as the main enemy, the Communist block ceased its existence. But there were also governmental comissions that, in the midd `90s advocated for an in-depth reform of the intelligence communities, envisioning some of the changes that the global and national security environment have undergone in the next decades to come. The reports[1] argued for the tapping of outside expertise, in order to enhance the Intelligence Community`s analytic capabilities, the creation of *Intelligence Civilian Reserves*, which should include former practitioners, scholars, representatives of NGOs or think tanks, or any other person holding a certain expertise, usefull in managing unanticipated crisis, in areas that do not represent a top priority for the intelligence agencies.

The second landmark we are reffering to is the 9/11 attacks. The events probably are the best illustration of the dark side of globalization and of the network society we are living in currently. Moreover, it underlined the need for a revolution in intelligence affairs (RIA), following the model of the revolution in military affairs. The 9/11 Comission, and many scholars in the field of intelligence and security studies, called for a re-thinking of intelligence, in all its dimensions. In what concerns the relationship with the Academia, the proposals put forward several years before were re-enhanced and were actually put into

[1] Twentieth Century Fund Task Force on the Future of U.S. Intelligence, *In from the Cold,* Washington: 1996. Permanent Select Committee on Intelligence, *IC21, the Intelligence Community in the 21st Century,* Washington: 1996. Commission on the Roles and Capabilities of the U.S. Intelligence Community, *Preparing for the 21st Century: an Appraisal of the U.S. Intelligence,* US: 1996.

practice. As Ruben Arcos[2] stated, a new intelligence function developed, that of managing trusted relationship with the Intelligence Community`s stakeholders, Academia included.

This paper will analyze the new intelligence paradigms and the role of Academia in supporting intelligence to aquire the knowledge needed to face current and emerging security threats. It will then underline the benefits and limits of academic outreach and present some outreach initiatives implemented in different democratic states. In the final part, we will asses the relationship between Academia and intelligence in Romania, focusing mainly on the Romanian Intelligence Service.

1. Shifting Paradigms. From Puzzles to Mysteries

Paraphrasing an old Chinese curse, there is no doubt that we are living in interesting times. Globalization, glocalization, regionalization, the free flows of people, trade, capital, information, the IT&C revolution, to name just a few elements, have influenced the international system, states and other actors. In almost a quarter of a century, since the end of the Cold War, much has changed on the international and national arenas.

As Keohane and Nye argued, the current international relations system is one that can best be characterized through their concept of *complex interdependence*. The concept refers to three dimensions, namely: (1) the use of multiple channels of action between societies in interstate, transgovernmental, and transnational relations, (2) the absence of a hierarchy of issues with changing agendas and linkages between issues prioritized and the objective of (3) bringing about a decline in the use of military force and coercive power in international relations.[3] As one can notice, these three elements have a direct linkage with the way a state should conduct its external and internal affairs, and thus the way governements take their decisions. As hard power declines, states are forced to appeal to soft power instruments and to the best knowledge intelligence agencies can offer them.

If the industrial era society, characterized by building things, was organized around hierarchies, the information era or the knowledge society manipulates information/intelligence/knowledge and is organized around networks. Power in the information age is based more on education, technology, and institutional adaptation than geography, population, or raw materials. Moreover, intelligence communities will rely more on information/knowledge, available from open sources, like the Internet and outside experts, than on secrets found through the usage of secret sources, to interpret world events and trends. One estimate is that *during the Cold War 80% of the information about the Soviet Union was secret and 20% was open, but in the post-Cold War period the ratio was more than reversed for Russia*. According to Mark Lowenthal, "this does not mean that classified collection disciplines are no longer needed, but that the areas in which OSINT is available have expanded.[4]

In this context, an increasingly number of scholars are sustaining the need for shifting the intelligence paradigm and are putting forward a series of models, that are usually based on dichotomies such as old paradigm vs. new intelligence paradigm, the liniar intelligence cycle vs. the network centric intelligence cycle, puzzles vs. misteries, traditional threats vs. transnational threats, etc.

---

[2] Ruben ARCOS, "Trusted Relationship Management as an Intelligence Function ", in Irena DUMITRU, Teodoru ȘTEFAN (ed.), *Intelligence in the Knowledge Society. Proceedings of the XVIII*th *International Conference,* Bucharest, Editura Academiei Naționale de Informații "Mihai Viteazul", 2013, pp. 61-74.

[3] Robert KEOHANE; Joseph NYE, *Putere și interdependență*, Polirom, Iași, 2009.

[4] Kenneth ROBERTS, *Better Analysis Through Networking: Expanding Outreach in an Era of Global Changes*, Paper presented at the International Studies Association Convention, Honolulu, Hawaii, March 4, 2005, available at http://www.scribd.com/doc/28736060/, accessed on 15.08.2014.

From Robert David Steele`s point of view, the differences between the old and the new intelligence paradigms are shaped by the evolution of threats to national security and by the adaptations intelligence agencies are required to implement in order to prevent and fight them. He argues that the disappearance of the old intelligence paradigm, and of the threats that characterized the Cold War period, has created the necessary space for the evolution of a new type of intelligence paradigm, namely, the *integrative* one. The new paradigm is ment to obtain a so called asymmetric advantage, both on the level of preventing and combating non-traditional threats, but also, in what concerns the usage of new intelligence sources and tehniques. Moreover, the new intelligence paradigm takes into account new types of threats resulting from the activity of non-state actors, which are non-conventional, unpredictible, unconstrained by any bounderies.[5]

The same Robert David Steele proposes the theory of the seven intelligence tribes. According to him, "*the traditional national intelligence tribe, the tribe of secret warfare and strategic analysis, will be joined by six other tribes, each of which will gradually assume co-equal standing in a secure global network: the military, law enforcement, business, academic, non-governmental and media, and religious or citizen intelligence tribes*". Moreover, in the near future, multi-lateral sharing rather than unilateral secrecy will be the primary characteristic of intelligence, as 80% of the value of intelligence will be in shared collection, shared processing, and shared analysis. Thus, intelligence is becoming *personal, public, and political*, being taught in schools and becoming a core competency of every knowledge worker.[6]

In explaining the differences between the old and new intelligence paradigms Gregory Treverton divides intelligence problems into *puzzles, mysteries and complexities.*
A *puzzle* in intelligence terms is primarily a challenge to collection. For instance, how many missiles did the Soviet Union possses during the Cold War period, represents a classic example of an intelligence puzzle. Puzzles have an answer, though we may not know it.

By contrast, *mysteries* are questions that cannot be answered with certainty. They are future and contingent. Collection is less crucial in this realm because information can only provide clues as to the likelihood of outcomes, not a definitive answer. [7] For mysteries, analyst usually rely on some history and sometimes on a certain theory, and thus some sense for what factors are important and how they will interact. From a similar perspective to that of Treverton, Schreier points out the fact that "*the major challenges of intelligence services now are more mysteries, often growing out of too much information with clues buried in too much "noise" and too many scenarios*". According to him, mysteries cannot be answered, instead they can be framed by identifying the critical factors and applying some sense of how they have interacted in the past and might react in the future. Solving puzzles is useful for detection, while framing mysteries is necessary for prevention and counteraction. The nature of such threats as terrorism, proliferation, and organized crime are predominantly mysteries, not puzzles and should be treated as thus.[8]

As for *complexities*, most likely, the analyst cannot rely on any of the above mentioned elements. Instead, many small actors may interact in ways that have not been seen

---

[5] Apud David STEELE, in Ionel Nițu, *Către o nouă paradigmă de intelligence?,* article published on the Intelligence Analysis Group, septembre 2014, available at https://www.facebook.com/groups/analiza/permalink/514395308697734/, accesed 25.08.2014.

[6] Robert David STEELE, ''Information Peacekeeping & the Future of Intelligence. 'The United Nations, Smart Mobs, & the Seven Tribes*" Peacekeeping Intelligence: Emerging Concepts for the Future*, Chapter 13, available at http://www.oss.net/.../file/Chapter%2013_Peacekeeping%20Intelligence.pdf, accessed 10.09 2014.

[7] Gregory TREVERTON, Foreword to *Sensemaking. A structure for an Intelligence Revolution*, in David Moore, *Sensemaking. A structure for an Intelligence Revolution,* Washington, National Defense Intelligence College Press, 2011, p. ix.

[8] Fred SCHREIER, *WMD Proliferation. Reforming the Security Sector to Meet the Threat,* Potomac Books, 2009.

before, and new ones will arise unpredictably. Thus, in theses cases, the best solution would be to work to resolve them toward mysteries, by providing structure as events develop, intelligence analyst becoming more and more ”sensemakers”. An example of this process is the Islamic terrorist threat. As Treverton argues, the years since 9/11 have added increasing intellectual structure to the problem, as we understand more about this unconventional threat - how terrorists are recruited, self-radicalization elements, the complex network structure of Al Qaeda and its various affiliates or sympathisers.[9]

In the new approach, the mission of intelligence is to perform *adaptive interpretations*[10] or, in Gregory Treverton's opinion to make the transition *from puzzle solving to sensemaking*. Adaptive interpretations involve constructing extremely complicated puzzles for which virtually all of the pieces are available. Furthermore, most pieces to these adaptive interpretations are not secrets or mysteries. Constructing adaptive interpretations is a two-step process. Both steps must be performed simultaneously and continuously. The necessary pieces of information must be procured and assembled into an accurate picture. Because these pieces of information come from sources across the globe, solving adaptive interpretations requires a very high level of prearranged information sharing[11].

Lahneman proposes the co-existence of two intelligence paradigms: the traditional one, to be used in cases that deal with predictable targets, and a new paradigm, based on adaptive interpretation and the usage of *trusted information*, a type of information that is nor secret, nor open. Moreover, he acknowledges that the solution to meeting the requirement of providing intelligence and warning for today's threats is the effective collaboration of state, local, tribal, and private sector entities in the collection of intelligence. Such cooperation means the sharing of large volumes of information, mostly open-sourced. At the same time, the IC would continue to use secret information from sensitive sources and methods.[12]

As one can observe, the effects of and responses to globalization have created a paradigm shift in the way information must be collected and processed. While traditional collection and analysis methods remain essential for certain information, issues magnified and expanded by globalization (terrorism, international crime, etc.) can only be understood by tapping the expertise of a variety of experts in the private sector. Much of the most useful information now exists in open sources. It needs to be captured, not duplicated or recreated. What is needed most urgently is help *sorting through the veritable flood of "readily available" information to identify what is relevant, and to clarify its implications*.[13]

Intelligence agency need to get out of their ivory tower, analyze the tasks that they can do on their own, and reach out to the Academia, private sector, civil society, external experts in one word for those tasks that can be done with their help. Tuomo Kuosa, in its Chapter entitled very poetical "*Fishing in the Pond of Borderless Risks and Threats*"[14], describes a situation quite similar to that of the intelligence tribes developed by Steele. He compares the security environment with a fish pond where risks and threats are the fish, and the organisations interested in identifing and preventing them are fishermen. These organizations "fish" for different types of knowledge with differnt instruments, from different angles and for different beneficiaries or reasons. But in the end, in order that the decisionmaker can take the best resolution, intelligence communities ough to integrate in their intelligence products

[9] Gregory TREVERTON, Foreword to Tuomo KUOSA , *Towards Strategic Intelligence – Foresight, Intelligence, and Policy-Making*, Dynamic Futures, 2014., pp. 7-8, available at http://ec.europa.eu/information_society/newsroom/cf/dae.
[10] Walter J. LAHNEMAN, "The Need for a New Intelligence Paradigm", *International Journal of Intelligence and Counterintelligence*, vol. 23, no. 2, (February 2010), p. 209.
[11] Walter J. LAHNEMAN. *Op. cit.,* p. 209.
[12] *Idem.*
[13] Kenneth ROBERTS, *Op. cit.,* p. 2.
[14] Tuomo KUOSA, *Op. cit.*

the perspectives of the other "fishermen", presenting them as alternative scenarios, thus letting the beneficiary to chose the best way of acting.

2. Bridging Intelligence and Academia. Benefits and Limits

The need for a closer relationship between intelligence communities and Academia is increasingly acknowledged by representatives of both media. The benefits of such an endeavour seem to be beneficial to both sides, although there are certain limits or hindrances, that appear to be accentuated in the case of ex-totalitarian states.

2.1 Benefits

Stephen Marrin, a former CIA analyst and current intelligence studies scholar, considers that Academia, and especially universities have the potential of adding value to the intelligence communities by acting as: a pool of graduates with substantial knowledge of use to the intelligence community; as a favorable milieu for a continuous training of intelligence officers; as an environment ready to pass on knowledge on specific topics from academic experts; as a forum which offers advice on intelligence reform, especially from those who specialize in intelligence issues; and, as a provider of graduates already at ease with tools and methods used in intelligence analysis.[15]

In its turn, Academia can benefit from the partnership as the IC: becomes an employer for some of their graduates; offers access to valuable data for scientific research, with the appropriate security clearances; can add more prestige to the universities, as it offers them the chance to support and inform intelligence beneficiaries; can offer financing, within the legal framework, both for universities, as research institutions, but also for certain representatives of the scholarly milieu.[16]

According to Lara Shohet[17], Academia have traditionally served intelligence in three principal ways: as sources of information, as contractors, and overseers and consultants of the IC. From this relationship stems a series of benefits for the both parts. In what concerns the IC, the main advantages would be:

- *Cost-efficiency* – by reaching to the Academia and the private research companies the IC is able to maintain advanced capabilities at a lower cost than if it had developed the technologies indoor. Moreover, by contracting out certain projects, the IC is free to choose the best specialists in the field.
- *Special expertise* – the number of analysts in any intelligence community is limited, and often one analyst has to focus on several topics at a time, as the agencies cannot afford to have very narrowly focused analysts. On the other hand, there are numerous academics that are studying an incredible spectrum of topics, often specializing in very narrow domains.

Their unique knowledge can offer the IC precious perspectives at one moment.

- *Public awareness* - As more academics have access to intelligence documents, they increase public awareness of the IC. Thus they can influence the public opinion about intelligence in a positive way and contribute to the development of a strong security culture. In evaluating intelligence work, they also provide unbiased and credible analysis of intelligence work. In addition, a review by top scholars and experts of intelligence products,

[15] Apud Stephen Marrin, in Valentin Fernand FILIP; Remus Ioan ŞTEFUREAC,"The Dilemmas of Linking Romanian Intelligence, Universities, and Think Tanks", *International Journal of Intelligence and Counterintelligence*, 2011, Vol. 24, No. 4, p. 717.

[16] Valentin Fernand FILIP, Remus Ioan ŞTEFUREAC, *Op. cit.*, p. 717.

[17] Lara SHOHET, "Intelligence, Academia and Industry," *The Final Report of the Snyder Commission*, Edward Cheng and Diane C. Snyder, eds., (Princeton Unversity: The Woodrow Wilson School of Public and International Affairs, January 1997) available at http://www.fas.org/irp/eprint/snyder/academia.htm., accesed 10.09.2014.

mainly with a strategic character, could add an extra credibility and even legitimacy to the activity of the intelligence community.
In what concerns scholars, the main advantages would be[18]:

- *Financial* – the IC can become an important source of financing for individual researchers, institutes or private companies. Although, probably, the payment would be less than in the private sector, involvment in such projects can bring researchers other non-financial payments.
- *Joint projects* – the IC and research and development companies/institutes are collaborating in developing dual-use technologies. Such projects enable industry to earn added profits by marketing variations of IC technology commercially. As a result, the IC can acquire technologies for less, and gains a "surge capacity". By using components, subsystems, and technologies developed by commercial industry in IC systems, it will be easier to build back capabilities to a higher level if necessary in the future.
- *Patriotic duty* – part of the outside experts gladly volunteer their services to the IC because they welcome the opportunity to serve their country.
- *Returning the favor* - in the course of its activities, intelligence has helped advance the interest of Academia and the private sector.
- *Being "inside"* – as former DCI Turner underlines, professors benefit from helping the IC because they get to see "*how governments really work*". If they act as consultants, professors may have access to classified information. Although they cannot reveal this information or use it in their teachings, professors may gain new insight into their field.

Moreover, the partnership with the IC gives academics the chance to have powerful influence, as they get to see their work having real-life implications in the undertakings of their government.

2.2. Limits and barriers

As Borchgrave et al. underlines, there are several deeply entranched obstacles that prevent meaningful collaboration for both the IC and outside experts. For the IC, these barriers include *legal, procedural, and professional issues*; *cultural biases*; *counterintelligence and deception concerns*; and the *inability to communicate topics of interest to academic and foreign audiences*. On the other hand, outside experts avoid collaboration with the IC due to concerns that doing so might *jeopardize their personal safety*; long-standing *professional norms* that discourage involvment with the IC; a *lack of government transparency* on how their information will be used; and a *one-way flow of information* wherein they provide insights and seldom receive any unclassified data in exchange.[19]

In the case of young democracies, which have undergone the experience of totalitarian regimes just a few decades ago, there is also a barrier between the IC and the outside experts, which stems from the remembrance of the political police activities undertaken by the predecesors of today's democratic intelligence agencies.

3. Academic Outreach Initiatives. The Romanian Case

Due to the limited space available we will describe very briefly the most important outreach initiatives implemented by some of the intelligence communities in the democratic

[18] *Ibidem.*

[19] Arnaud de BORCHGRAVE, Thomas SANDERSON, David GORDON, *The Powerof Outreach. Levereaging Expertise On Threats in Southeast Asia,* Center for Strategic and International Studies, Washington, 2009, p. xi, available at http://csis.org/files/media/csis/pubs/090430_deborchgrave_poweroutreach_web.pdf, accesed 12.09.2014.

world. One must mention, though that these type of activities are influenced by the state`s tradition, the resources available and that the U.S. is often a model for other smaller countries.

The *U.S.* has a long standing tradition in tapping outside expertise, especially as consultants or reviewers. But the first step towards institutionalizing what is called analytic/academic outreach is the U.S. Intelligence Community Directive no. 205[20], effective as of 16 July 2008, that defines analytic outreach as „*the open, overt, and deliberate act of an IC analyst engaging with an individual outside the IC to explore ideas and alternate perspectives, gain new insights, generate new knowledge or obtain new information.*" As for the practices used, we can find all the forms identified by Treverton[21]: co-production of intelligence products; virtual co-production, using blogs or wiki technologies; outsiders on retainer for occasional analysis or consultation (*NIC Associates, IC Associates*); joint working groups on specific topics; ongoing collaboration on methods (*Global Futures Forum*); publications targeted or available to outsiders (*Studies in Intelligence*); conferences opened to outside experts, and the usage of web sites to invite tips or other information. Moreover, the IC has sponsored analysts to go an teach at top universities through its *Officer in Residence Program.*

Canada, through the Canadian Security Intelligence Service (*CSIS*) launched its *Academic Outreach Program,* as an attempt to better link academic work with the intelligence domain. Its main objectives are: to create awareness within Canadian academics of CSIS priorities; to contribute to a better informed public discussion of security in the country; and to draw from the expertise generated in the realm of research on security issues and to bring that knowledge to bear on CSIS investigations. This task is carried out by building context around investigative topics that challenge the understanding that analysts and collectors have of those issues. The knowledge gathering methods of Academic Outreach contain workshops, conferences, expert briefings, interviews, and commissioned studies. As *CSIS* underlines „*the activities aim to develop a long-term view of various trends and problems, to challenge our own assumptions and cultural bias, as well as to sharpen our research and analytical capacities."*[22]

In the case of *Spain, the CNI (Centro Nacional de Inteligencia)* launched an Intelligence Culture Initiative in the mid 2000s aimed to allow the services to reach out for expertise to academic scholars and non-IC stakeholders, including the private sector. Apart from publications, conferences, workshops, the *CNI* signed agreements with different Spanish universities and launched an MA in intelligence analysis. The initiative lead to a development of Intelligence Studies literature and of the field as an academic and research discipline.[23]
In the case of *Romania,* up to the current moment there is no initiative officially launched to enhance the cooperation between the academic milieu and the IC. However, most of the institutions that make up the IC are reaching out to outsiders through their dedicated publications, conferences, workshops.

As for the *SRI*, one can identify several steps that have been made thus far in order to fill in the gap between Academia and the IC. Unlike other states the SRI has a unique component, the *National Intelligence Academy,* a research and learning university that acts as

[20]Director of National Intelligence, *IC Directive no. 205 – Analytic Outreach,* available at http://www.dni.gov/electronic_reading_room/ICD%20205.pdf.
[21] Gregory TREVERTON, *Approaches to "Outreach" for Intelligence,* The Swedish National Defence College, 2009, available at https://www.fhs.se/Documents/Externwebben/nyheter/2009/approaches-to-outreach-for-intelligence.pdf., accessed 10.09.2014.
[22] For more details on the Program see https://www.csis.gc.ca/bts/cdmctrch-en.php, and Louise DOYON, "*One Year Through: Taking Stock of the Canadian Security Intelligence Service (CSIS)'s Program of Outreach to Experts*", paper presented at the International Studies Association Convention, New Orleans, 2010, available at https://www.csis.gc.ca/pblctns/wrldwtch/2010/takngstck-en.php.
[23] For more details on the Initiative see Ruben ARCOS, *Op. cit.*

a genuine research hub. The NIA trains the future and current officers of the IC and also offers masters and PhD programs to the civils interested in intelligence studies. These programs address specific stakeholders and future decisonmakers, thus helping to establish a stronger security and intelligence culture at the level of the Romanian society. Moreover, through its research branch, the *National Institute for Intelligence Studies (INSI),* the

Academy is networking with researchers from the national and international arena and is developing national and european scale research projects.

Moreover, the SRI signed an agreement with the University of Bucharest and in 2008 launched an MA in intelligence analysis.

The importance of the Academia as a partener of intelligence agencies has been underlined by the strategic documents ellaborated at the level of the SRI (such as the Strategic Vision) and by the Service's leadership. In 2008 George Maior, the Director of the SRI , stressed „*that it is extremely important for an intelligence agency to be able to work and interact with academic and professional analysis centres in order to offer decisionmakers the intelligence needed to take the most accurate and timely decisions in the national security field*". The support of the top management is allways a favourable and neccesary condition for the succes of any initiative to change the culture of an organization.

Conclusions

By tapping outside expertise the intelligence communities will manage to *sail on the ocean of OSINT*, to develop the skills of their employees and enhance their anlytic capabilities, to build an intelligence culture at the level of the society, to draw on very specialized expertise and to cover more of the potential threats. Outreach may reduce costs, improve the public perception of the IC, and even help to educate the current and future beneficiaries. The benefits are selfevident. But strengthening the relatinoship with Academia means opening up, building trust and changing some of the biases that can be found inside intelligence organizations.

Acknowledgement:

This paper is made and published under the aegis of the Research Institute for Quality of Life, Romanian Academy as a part of programme co-funded by the European Union within the Operational Sectorial Programme for Human Resources Development through the project for ***Pluri and interdisciplinary in doctoral and post-doctoral programmes Project Code: POSDRU/159/1.5/S/141086.***

BIBLIOGRAPHY:

1. ARCOS, Ruben, "Trusted Relationship Management as an Intelligence Function", in Irena DUMITRU, Teodoru ŞTEFAN (ed.), *Intelligence in the Knowledge Society. Proceedings of the XVIIIth International Conference*, Bucharest, Editura Academiei Naţionale de Informaţii "Mihai Viteazul", 2013, pp. 61-74.
2. BORCHGRAVE, Arnaud de; SANDERSON, Thomas; GORDON, David; *The Powerof Outreach. Levereaging Expertise On Threats in Southeast Asia,* Center for Strategic and International Studies, Washington, 2009, p. xi, available at http://csis.org/files/media/csis/pubs/090430_deborchgrave_poweroutreach_web.pdf.
3. DOYON, Louise. "One Year Through: Taking Stock of the Canadian Security Intelligence Service (CSIS)"s Program of Outreach to Experts", paper presented at

International Studies Association Convention, New Orleans, february 2010, available at https://www.csis.gc.ca/pblctns/wrldwtch/2010/takngstck-en.php.
4. FILIP, Valentin Fernand; ŞTEFUREAC, Remus Ioan,"The Dilemmas of Linking Romanian Intelligence, Universities, and Think Tanks", *International Journal of Intelligence and CounterIntelligence*, 2011, Vol. 24, No. 4, pp. 711-732, DOI: 10.1080/08850 607.2011.598790.
5. KEOHANE, Robert; NYE, Joseph, *Putere Şi interdependenţă,* Polirom, IaŞi, 2009.
6. KUOSA, Tuomo, *Towards Strategic Intelligence – Foresight, Intelligence, and Policy-Making,* Serial: Dynamic Futures Publications No. 1, Published by: Dynamic Futures, 2014.
7. LAHNEMAN, Walter. "The Need for a New Intelligence Paradigm", International Journal of Intelligence and Counterintelligence, vol. 23, no. 2, (February 2010)
8. ROBERTS, Kenneth, *Better Analysis Through Networking:Expanding Outreach in an Era of Global Changes,* Paper presented at the International Studies Association Convention, Honolulu, Hawaii, March 4, 2005, available at http://www.scribd.com/doc/28736060
9. SHOHET, Lara, "Intelligence, Academia and Industry," *The Final Report of the Snyder Commission*, Edward Cheng and Diane C. Snyder, eds., (Princeton Unversity: The Woodrow Wilson School of Public and International Affairs, January 1997) available at http://www.fas.org/irp/eprint/snyder/academia.htm.
10. TREVERTON, Gregory, *Approaches to „Outreach" for Intelligence*, The Swedish National Defence College, 2009, available at https://www.fhs.se/Documents/Externwebben/nyheter/2009/approaches-to-outreach-for-intelligence.pdf.
11. TREVERTON, Gregory. Foreword to *Sensemaking. A structure for an Intelligence Revolution*, by David Moore, Washington: National Defense Intelligence College Press, 2011.

MERCENARY OR PRIVATE CONTRACTOR? LEGAL PROVISIONS ON PRIVATE MILITARY COMPANIES.

Tiberiu POPA
Lieutenant Col., AD ROU Army, PhD candidate within "International Relations and Security Studies" Doctoral School, "Babes-Bolyai" University, Cluj Napoca, Romania.
E-mail address: popa.ctiberiu@gmail.com

Abstract: *The end of the XX century and the beginning of the XXI century witnesses deep transformations in the global security. The transition from bipolarity to multipolarity and the extension of the corporatization into the fields other than the economic one, with the main vector of spread the globalization phenomenon, have changed the security into a common commodity, which can be dealt with as with any other economic good, through the prism of supply and demand, as well as the profit margin. Within this context, the traditional actors of the security environment (global and regional security organizations and the national states) had to allow the existence of some new actors, as the private military and security companies. They have undertaken military functions whose monopoly was held, until recently, by the national States and have greatly developed, mainly due to the armed conflicts from the beginning of this century, which generated the demand, and the lack of a coherent legal framework to globally regulate the activities of these companies, which acted as a catalyser. The challenges due to the development of this phenomenon have been generated on multiple fields: ethical, moral, economic, legal, etc.; amongst them, the similarity of the Private Military Companies (PMC) phenomenon with the mercenarism is not to be disregarded. The article analyzes the international legal framework in this field and aims to find useful conclusions for defining and framing this phenomenon.*

Keywords: *private military companies (PMC), international law, mercenary.*

Introduction

The end of the Cold War, period which has led to an increase in military spending at considerable levels, has led to their collapse, under the circumstances in which the security environment was rebuilt. The transition from bipolarity to multipolarity, with a short period of time of unipolarity at the end of the last decade of the last century, has also witnessed the diminishing of the national armies' budgets. More than that, the economic fluctuations have emphasized this trend; thus, the outsourcing seemed to the most logical way to go ("When an entire industry exists to run warehouses efficiently, why do we own and operate so many of our own? At bases around the world, why do we pick up our own garbage and mop our own floors, rather than contracting services out, as many businesses do?")[1] . From here to the state's coercion monopoly outsourcing there was one step only. However, this step had been already done through the activities of some PMCs as Executive Outcomes, in 1995, in Sierra Leone[2].

[1] RUMSFELD, Donald, US DOD secretary - DOD Acquisition and Logistics Excellence Week Kickoff – Bureaucracy to Battlefield, 10.09.2001, at http://www.defense.gov/Speeches/Speech.aspx?SpeechID=430, on 10.07.2014.
[2] SINGER, Peter W.- Corporate Warriors: The Rise of the Privatized Military Industry, Cornell University Press, 2003, p. 4-5.

1. Mercenarism throughout the history

This transition of an essential military function through a commercial entity rose not moral dilemmas only, but legal ones too. The similarity with the mercenarism likely is the most obvious. The most common definition of a mercenary is that of a person employed for its military skills in a foreign army. Similar definitions show the mercenary as a person selling his military skills to the highest bidder. Without looking for an exhaustive definition, we can easily see that this phenomenon is not a new one. The author Peter W. Singer wrote that it is "as old as war"3. In fact, a retrospective view on the mercenary easily comes to the conclusion that the phenomenon has accompanied the mankind from the oldest times to nowadays. Thus, the oldest mentioning of mercenary belongs to King Shulgi of Ur (2094-2047 î.C.)4. Soldiers fighting for profit could be found in 1274 b. C., working for Ramses II against Hittite king Muwatali[5], in the battle of Qadesh.

The Greek city-states have frequently used rented soldiers, be them Cretan slingers, Syracusan hoplites or Thessalian cavalry6. For the Roman Empire, its army composed of citizens was not enough, so mercenaries from the occupied territories have been employed. Similarly, the Byzantine Empire has greatly used the services of the Grand Catalan Company. During the Middle Age, pikemen companies have sold their expertise to the highest bidder. The abundance of mercenary supply had been so big, that the King Charles VII of France has included the most part of them in a standing army, at the middle of the XVth century. Those remaining not included migrated to the Italian cities, joining the already famous "condottieri". The Suisse Guards of the Papacy are also mercenary with a long tradition. Up to the signing of the Westphalian Treaties, the mercenaries ensured the supply of military services and stimulated the demand, thereby making a perpetual war.

Later on, commercial non-state entities have appeared, endowed with the right of bearing wars. For example, the Dutch East India Company had the right of making war, issuing the currency, jailing and even executing detainees[7]. Similar rights have been granted to its main rival, the British East India Company. Even their main role was an economic one, to reach their objectives they were entitled to bear own local wars, sometimes using more soldiers than available in their origin countries.

Decolonization from the beginning of the 20th century witnessed the appearance of the individual mercenaries, fighting especially in the conflicts related to auto determination but the existence of private companies, as well. A closer example is Executive Outcomes Company (South Africa), which has undertaken military actions in Angola (1994) and in Sierra Leone (1995).

A preliminary conclusion is that the mercenarism is not something new in history; au contraire, its existence accompanied the mankind from the oldest times. The change of the international relations system creates a security dilemma through the existence and activities of the PMC, based on purely economic principles. Therefore, a global regulation of the phenomenon is greatly needed.

---

[3] SINGER, Peter W - Corporate Warriors: The Rise of the Privatized Military Industry, Cornell University Press, 2003, p. 19.

[4] THOMSON, Janice - Mercenaries, Pirates and Sovereigns: State Building and Extraterritorial Violence in Early Modern Europe, Princeton University Press , 1996, p.15.

[5] DUPUY, Richard Ernest, Dupuy, Trevor N. - The Encyclopedia of Military History from 3500 B.C. to the Present, 2nd Revised Edition, Harper & Row Publishers, 1986, p. 22.

[6] Singer, Peter W.- Corporate Warriors: The Rise of the Privatized Military Industry, Cornell University Press, 2003, p. 21.

[7] GARETT, Allison, Corporations as Sovereign, în Maine Law Review 2008, p. 133, at http://mainelaw.maine.edu/academics/maine-law-review/pdf/vol60_1/vol60_me_l_rev_129.pdf, on 29.07.2013.

2. Mercenaries. Legal provisions of the international law treaties

We have come to the conclusion that the mercenarism is very old and that it needs global regulation. Measures have been taken recently and provisions have been given to define the mercenarism as a crime. Thus, the Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, stipulates the cumulative conditions that a person must fulfil in order to be considered a mercenary. According to its 47 article, a mercenary is any person who:

a. is specially recruited locally or abroad in order to fight in an armed conflict;
b. does, in fact, take a direct part in the hostilities;
c. is motivated to take part in the hostilities essentially by the desire for private gain and, in fact, is promised, by or on behalf of a Party to the conflict, material compensation substantially in excess of that promised or paid to combatants of similar ranks and functions in the armed forces of that Party;
d. is neither a national of a Party to the conflict nor a resident of territory controlled by a Party to the conflict;
e. is not a member of the armed forces of a Party to the conflict; and
f. has not been sent by a State which is not a Party to the conflict on official duty as a member of its armed forces[8].

The mercenary is also defined in The African Convention for the Elimination of Mercenarism in Africa, signed in Libreville on 3 July 1977 and entered into effect on 22 April 1985. The definition is similarly shaped as the one in the Protocol I to the Geneva Convention. Thus, mercenary is any person who:

a. is specially recruited locally or abroad in order to fight in an armed conflicts;
b. does in fact take a direct part in the hostilities;
c. is motivated to take part in the hostilities essentially by the desire for private gain and in fact is promised by or on behalf of a party to the conflict material compensation;
d. is neither a national of a party to the conflict nor a resident of territory controlled by a party to the conflicts;
e. is not a member of the armed forces of a party to the conflict; and
f. is not sent by a state other than a party to the conflict on official mission as a member of the armed forces of the said state[9].

It is easy to notice that the difference between the definitions is to be found at the third criteria, where OAU Convention does not make any difference in what concerns the size of the private gain, when compared to that of the similar ranking members of the armed forces. These conditions are also cumulative. Also, the Convention not only defines the mercenary as individual but stipulates the conditions to be met for a group or association or even a state to be considered guilty of mercenarism.

[8] https://www.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument&documentId=9EDC5096D2C036E9C 12563CD0051DC30, on 29.07.2014.
[9] https://www.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument&documentId=A8AB2D0B83BD8AA5C12563CD0051EB19, on 29.07.2014.

The third definition is to be found in the International Convention against the Recruitment, Use, Financing and Training of Mercenaries, 4 December 1989.

According to its provisions, a mercenary is any person who:

a. Is specially recruited locally or abroad in order to fight in an armed conflict;
b. Is motivated to take part in the hostilities essentially by the desire for private gain and, in fact, is promised, by or on behalf of a party to the conflict, material compensation substantially in excess of that promised or paid to combatants of similar rank and functions in the armed forces of that party;
c. Is neither a national of a party to the conflict nor a resident of territory controlled by a party to the conflict;
d. Is not a member of the armed forces of a party to the conflict; and
e. Has not been sent by a State which is not a party to the conflict on official duty as a member of its armed forces.

2. A mercenary is also any person who, in any other situation:

a. Is specially recruited locally or abroad for the purpose of participating in a concerted act of violence aimed at:
   (i) Overthrowing a Government or otherwise undermining the constitutional order of a State; or
   (ii) Undermining the territorial integrity of a State;
b. Is motivated to take part therein essentially by the desire for significant private gain and is prompted by the promise or payment of material compensation;
c. Is neither a national nor a resident of the State against which such an act is directed;
d. Has not been sent by a State on official duty; and
e. Is not a member of the armed forces of the State on whose territory the act is undertaken[10].

Again, the pattern of the Protocol I can be noticed. The main difference resides in the fact that taking part in hostilities is not a condition to be met anymore. Instead, the domain is now extended with the participation to any act of violence, which is not necessarily an international conflict. Thus, included in the definition are the persons who participate in overthrowing governments or undermining the constitutional order of a state or its territorial integrity.

It can easily be seen the difficulty of cumulatively joining all the conditions to label a person as mercenary. It is likely the reason that stands behind the statement of Geoffrey Best, according to whom "any mercenary who cannot exclude himself from this definition deserves to be shot and his lawyer with him! [11]"

It is worth mentioning that these legal provisions are not applicable to all states. Thus, the Protocol I has been ratified by 174 states, with 3 of them only signing it, U.S.A., Pakistan and Iran. The OAU Convention for the Elimination of Mercenarism in Africa has been ratified by 30 states, with 15 of them signing only. Similarly, the International Convention against the Recruitment, Use, Financing and Training of Mercenaries has been ratified by a number of 33 states and signed by 10 states, with the most notable exceptions U.S.A. and the U.K., two important actors in the field of PMC. Therefore, to the intrinsic difficulty of the legal framework it can be added the challenges generated by the very difference of actors of

[10] http://www.un.org/documents/ga/res/44/a44r034.htm, on 19.08.2014.

[11] Geoffrey BEST, - Humanity in Warfare: The Modern History of the International Law of Armed Conflict, Littlehampton Book Services Ltd, 1980, p. 328, note 83.

the security environment. Further, we will analyze the difficulty of having all the conditions cumulatively met by the PMC personnel.

3. Mercenary or private contractor?

From the international law point of view, the PMCs belong to a blurred frontier area, in the way that they represents economic entities, acting according to the supply and demand requirements but earning profits from military activities, traditionally reserved to the national states. As a result, the profit race creates security dilemmas, these companies acting outside the international law framework.

The first criterion defining the mercenary is the fact that he *is specially recruited locally or abroad in order to fight in an armed conflict*. The private contractors are individuals employed by a company and having a legal employment contract. The international law does not include within the definition of mercenary companies, societies, firms, but individuals only; therefore, the private contractors can be easily excluded from the definition. More than that, their contracts include tasks referring to the persons and assets protection and security. In the conflict areas, these tasks could easily go beyond this point and transform in armed conflict. The difference between protection (fulfilling tasks) and armed conflict is hard to observe. Additionally, the individual contract provisions are hardly public available.

*Taking part in hostilities*_is the second criterion to be fulfilled by a person to be labelled as mercenary. Both the 47th article of the Protocol I and 1st article of the UN Convention include "taking part in hostilities" words; however, this collocation is not defined in the international law. Nevertheless, the International Committee of the Red Cross has issued guidance for interpreting this notion, which consists of three elements:

1. The act must be likely to adversely affect the military operations or military capacity of a party to an armed conflict or, alternatively, to inflict death, injury, or destruction on persons or objects protected against direct attack (threshold of harm), and
2. There must be a direct causal link between the act and the harm likely to result either from that act, or from a coordinated military operation of which that act constitutes an integral part (direct causation), and
3. The act must be specifically designed to directly cause the required threshold of harm in support of a party to the conflict and to the detriment of another (belligerent nexus) [12].

This guidance is not an international law provision but a recommendation to be followed, which is based on the vast knowledge of a great number of experts in this field.

The desire of private gain is a criterion which is present in all analyzed norms. However, the same motivation can be seen also to the Armed forces members, the only difference being the amount of gain. This problem had been also analyzed by the House Committee on Oversight and Government Reform[13], where has been observed that the income of a private contractor is six to nine time the income of an Army sergeant. Even though the amount of income is very different from a company to another and amongst different employees, there are numerous facts and statements supporting the idea of the private gain as

[12] MELZER, Nils - Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law, page 56, at https://www.icrc.org/eng/assets/files/other/icrc-002-0990.pdf, on 09.09.2014.

[13] House Committee On Oversight And Government Reform - Hearing on Private Security Contracting In Iraq And Afghanistan, October 2, 2007, available at http://www.washingtonpost.com/wp-srv/politics/articles/blackwater_hearing_100207.html, on 19.08.2014.

a reason that stands behind the employment. ("For money, obviously! Anyone saying anything else is shamelessly lying") [14].

The nationality and the citizenship are features invoked to build the forth criterion. In Iraq, a part of the private contractors were Americans or British, their countries being party of the conflict; thus, they could not be considered mercenary. The Iraqis, employees of the same company, were seen as members of the other party of the conflict, thereby making this criterion useless. The Hondurans, Fijians or any other states, non-members of the Coalition would fit the definition of the mercenary but this thing is easily avoidable by giving them the citizenship of a country member of the conflict.

Not being a member of the armed forces of a party to the conflict or of any other state, third party, sent in official mission lead to the idea that all employees of a private military company would fall within the definition of the mercenary. However, this criterion is also easily disabled, by incorporating the employees of the company or even the whole company within the regular armed forces. A precedent had already been created, when the Sandline International employees have received the status of "Special Constables[15]" of the Papua New Guinea state, thereby disabling the mercenary status.

Conclusions

We have concluded by now the fact that the mercenarism is an old activity, which accompanied the mankind throughout the history up to nowadays and that has become intolerable only in the last century.

Further, in the recent days, the international security organizations have been adopted legal provisions, due to forbid the mercenarism and the use of the mercenaries for solving their problems.

Also, we have shown that these legal provisions cannot strictly frame the phenomenon of mercenarism; therefore, PMCs and their employees, which present striking similarities with the mercenarism, cannot legally be declared mercenary.

Considering the challenges raised by the very existence of these PMC, as well as the legally gray border zone in which they operate, the solution can be a new U.N. Convention to globally regulate the legal working framework of them. This way, the already existing Draft of a possible Convention on Private Military and Security Companies (PMSCs) for consideration and action by the Human Rights Council[16] is a good start, which needs to be amplified and ratified by all states.

Acknowledgement:

This work was possible with the financial support of the Sectoral Operational Programme for Human Resources Development 2007-2013, co-financed by the European Social Fund, under the project number POSDRU/159/1.5/S/138822 with the title ***"Transnational network of integrated management of intelligent doctoral and postdoctoral research in the fields of Military Science, Security and Intelligence, Public order and***

[14] Vlad, TEODORESCU, Secretele unui mercenar roman în Irak, Evenimentul Zilei, 16 ianuarie 2013, la http://www.evz.ro/un-interviu-in-exclusivitate-pentru-evenimentul-zilei-secretele-unui-mercenar-roman-in-ir-101945.html, on 19.08.2014.

[15] Sturzaker, Damian, Cawood, Craig - The Sandline Affair. Illegality and International Law, in Australian Intemational Law Jurnal, 1999, pag. 215,la http://www.austlii.edu.au/au/journals/AUIntLawJl/1999/13.pdf,, on 19.08.2014.

[16] http://www2.ohchr.org/english/issues/mercenaries/docs/A.HRC.15.25.pdf, on 19.08.2014.

BIBLIOGRAPHY:

1. BEST, Geoffrey - Humanity in Warfare: The Modern History of the International Law of Armed Conflict, Littlehampton Book Services Ltd, 1980.
2. DUPUY, Richard Ernest DUPUY, Trevor N. - The Encyclopedia of Military History from 3500 B.C. to the Present, 2nd Revised Edition, Harper & Row Publishers, 1986
3. SINGER, Peter W. - Corporate Warriors: The Rise of the Privatized Military Industry, Cornell University Press, 2003.
4. THOMSON, Janice - Mercenaries, Pirates and Sovereigns: State Building and Extraterritorial Violence in Early Modern Europe, Princeton University Press, 1996.
5. Draft of a possible Convention on Private Military and Security Companies, at
6. http://www2.ohchr.org/english/issues/mercenaries/docs/A.HRC.15.25.pdf
7. Garett, Allison - Corporations as Sovereign, în Maine Law Review 2008 at http://mainelaw.maine.edu/academics/maine-law-review/pdf/vol60_1/vol60_me_l_rev_129.pdf
8. House Committee On Oversight And Government Reform - Hearing on Private Security Contracting In Iraq And Afghanistan, October 2, 2007, at http://www.washingtonpost.com/wp-srv/politics/articles/blackwater_hearing_100207.html
9. International Convention against the Recruitment, Use, Financing and Training of Mercenaries, 4 December 1989 at http://www.un.org/documents/ga/res/44/a44r034.htm
10. Melzer, Nils - Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law, at https://www.icrc.org/eng/assets/files/other/icrc-002-0990.pdf
11. OAU Convention for the Elimination of Mercenarism in Africa. Libreville, 3rd July 1977 at www.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument &documented=A8AB2D0B83BD8AA5C12563CD0051EB19
12. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977 at www.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument&documentId=9EDC5096D2C036E9C12563CD0051DC30;
13. RUMSFELD, Donald - DOD Acquisition and Logistics Excellence Week Kickoff – Bureaucracy to Battlefield, 10.09.2001, at http://www.defense.gov/Speeches/Speech.aspx?SpeechID=430,
14. STURZAKER, Damian, Cawood, Craig - The Sandline Affair. Illegality and International Law, in Australian Intemational Law Jurnal, 1999 at http://www.austlii.edu.au/au/journals/AUIntLawJl/1999/13.pdf,
15. TEODORESCU, Vlad - Secretele unui mercenar roman în Irak, Evenimentul Zilei, 16 ianuarie 2013, at http://www.evz.ro/un-interviu-in-exclusivitate-pentru-evenimentul-zilei-secretele-unui-mercenar-roman-in-ir-101945.html

CONSIDERATIONS ON NATIONAL COMBAT EVALUATION CENTRE ACCREDITATION AND FUNCTIONALITY

Jan-Florin GANEA
Lieutenant-colonel, Superior instructor, Armour Training Centre Piteşti,
PhD candidate in Military Science at "Carol I" National
Defence University Bucharest, Romania.
E-mail address: jganea@yahoo.com

Abstract *The combat readiness evaluation CREVAL, the official evaluation tool of NATO response forces (NRF[1]) land component, is known to a limited number of professionals, because the specific training is costly and it is only performed under ACO[2] supervision, in NATO School Oberammergau, Germany. In order to acquire a higher efficiency at national level, the author suggest the articulation of a small, supple and mobile structure designed for manning the evaluation teams and the CREVAL training of decision makers, key personnel and lower level military management of the Romanian Land Forces, as part of the multi-service evaluation body.*

Keywords: *land forces, operational evaluation, CREVAL, national centre, response force, NRF.*

Introduction

The feature that brings together those 28 countries composing the North Atlantic Treaty Alliance is the concept of collective defence. As a result, the allied militaries developed cooperation programmes facilitating the joint synergy of all actionable components, concept known as interoperability. The interoperability is the capability that allows the military structures to act together in order to commonly achieve the designated tasks. In the same time, the interoperability spans on a wider scale of shades, representing, in the early stages, the initial harmonization requirement aiming on allied forces cohesion. Semantically speaking, the interoperability exists when two or more sides have the same representation regarding a phenomenon, concept or action. On the other side, the basic understanding alone cannot guarantee the harmonization of force generation, the training and the combat use of NRF forces.

Until the 90s, the view on the operational evaluation was a heterogeneous one, because the objectives were common, but every allied nation applied its own set of evaluation standards. After the year 2000, the alliance initiated a formal process of elaboration of a unique evaluation system, primarily designed for NRF. The need was triggered by the size reduction of forces, as the politico-military situation was considered strong enough to manage the power equation worldwide. Also, from the legitimacy point of view, the NRF had to incorporate contingents from all the allied member nations, thus putting pressure on the necessity of full scale interoperability. The task of this common evaluation system was given to a collective body, coordinated by specialists from training and exercises structure from

[1] NATO Response Force, in accordance with NATO Terms and Definitions, AAP-006, Edition 2009.
[2] Allied Command Operations, located in Mons, Belgium.

SHAPE[3]. The group included officers from the entire NATO command structure[4] of that time. The result, regarding the land forces evaluation, was the Combat Readiness Evaluation (CREVAL) manual, officially introduced in use in 2009, after one year probation period.

1. The CREVAL training nowadays

From the very moment of introduction of the newer evaluation system, the concerned decision makers had to decide also on the ways of supporting the popularization of it. In order the system to work properly, new generations of evaluators and training audience key personnel had to be trained in the new subject. It was not a complicate concept, particularly because it melted together principles and operational procedures from the expertise of a significant number of allied nations, older or newer in the alliance.

The solution chosen was two yearly courses, lasting one week, preceded by a trainer's workshop for another week, for the course setting and technical improvement of the evaluation manual, based on the latest lessons learned collected from the nations. The Allied Command Transformation[5] set the location of this course in NATO School Oberammergau[6]. The course was taught by NCS officers with duties in the land forces evaluation, respectively two officers from ACO and one from each component command land (CC-Land) HQ, in Madrid and Heidelberg respectively. Still, the number of trainees, about 40 per each course iteration, was insufficient, and therefore ACO accepted the two CC-Land HQs, Madrid and Heidelberg, to organise their own annual CREVAL course, thus bringing an addition of 40 trainees, mostly from the respective headquarters. Moreover, after Croatia and Albania joined the Alliance, NSO organised, based on Croatia request, an ad-hoc CREVAL course at the Croatian Defence Academy in Zagreb. This iteration brought yearly, from 2009, some other 50 graduates, mainly from the host country and the surrounding allied and partner nations.

The course was based on an arrangement between NSO and Croatian MoD[7], where the host offered the training premises. The course was approved for a number of PfP[8] nations (European PfP nations plus Georgia, Armenia and Azerbaijan), because starting with 2006, the interim CREVAL procedure was introduced in the evaluation of PfP troop contributing nations (TCNs) to NATO operations.

2. The Execution of CREVAL Evaluations in the Romanian Army

Starting with 2004 the year Romania joined the North Atlantic alliance, it was introduced, experimentally, the interim evaluation manual.

In the Romanian Army, the Interim Forces Standards (IFS) started to be slowly introduced in practice, initially in the units designated for abroad NATO theatres of operations. At that time, Romania was on the verge of performing the NATO evaluations properly, with the corps of trainers that it had.

[3] Supreme Headquarters Allied Powers Europe, also known as ACO – Allied Command Operations, located in Mons, Belgium.
[4] NCS – NATO Command Structure, in accordance with AAP-006.
[5] ACT, located in Norfolk, VA, USA.
[6] NSO, located in Oberammergau, Germany, allied institution sponsored by USA and Germany.
[7] Ministry of Defence, as per AAP-006.
[8] Partnership for Peace, NATO initiative launched in 1994, aimed at creating trust between NATO and other states in Europe and the former Soviet Union; 22 states are members, first one that applied for was Romania.

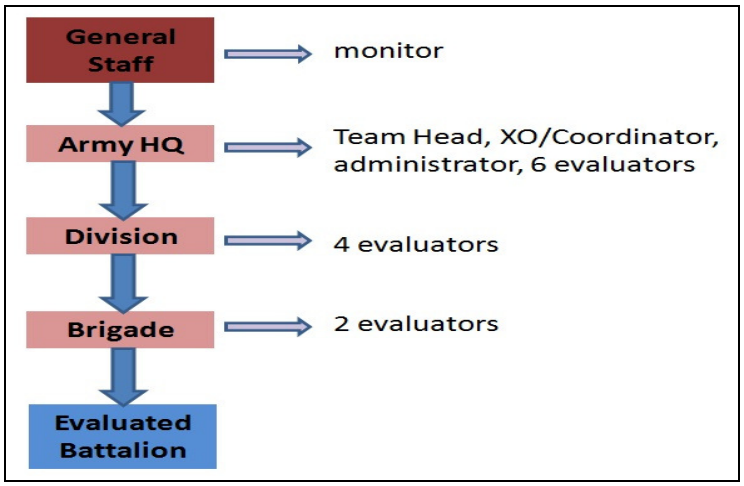


Figure no. 1. Possible composition of evaluation team for land forces

It was a priority to develop a reasonable number of trained personnel, in order to manage decently the compatibility issues in regard to national troops participation in the areas where Romania assumed responsibilities, meaning in the NATO theatres, Iraq, Afghanistan, and the Balkans. Moreover, since the initial introduction of interim evaluation standards, the national military authorities were requested opinions on improvement of the evaluation tool, on the same basis of fairness and transparency, and this was not possible since the number of end users was so limited. Subsequently, the personnel structure from Romanian MoD selected and sent to the CREVAL course in NSO officers to each of the two annual iterations, starting with 2006. Romania also sent officers for the internal CREVAL courses conducted in CC Land HQ Madrid, due to the operational geographical affiliation. In addition to this, in the summer of 2007, representatives from CC-Land HQ Madrid were invited by Romanian General Staff to present a sequence of lectures in order to detail the CREVAL evaluation procedure. For almost a week, they addressed to 53 fellow national officers, clearing the path to understand the intimate reasons and procedures of CREVAL. Today, after having an important number of officers trained in CREVAL field, less than a quarter are available for operational evaluations, due to career personnel moves (promotions, change of expertise field, retirement etc). Meantime, the CREVAL endeavours were conducted by teams composed of Land Forces Command (Army HQ) officers, with a core consisting of formally trained personnel and with proper expertise in the evaluated areas, as presented in Figure 1. Still, the problem was that these officers were selected from different echelons subordinated to the Land Forces Command, thus being exposed to the risk of fraternization with the training evaluated audience. On the other side, the team was articulated just weeks in advance, lacking cohesion and horizontal cooperation experience in CREVAL field, with the exception of a core of 3-4 members normally used in similar challenges.

3. Accreditation of the National Combat Evaluation Centre

The evaluation issue is a delicate one on any concerned field of activity. In Romania, it created controversies, for instance, in the public education academic level. The high school finalization and the admission in the universities are performed based on a specific evaluation, tailored on the profile and level of ambition of the education institution. Aiming at harmonization of evaluation process, and also on its transparency and predictability, the Ministry of Education proposed the foundation of National Evaluation and Examination Centre (NEEC), a structure specialised in educational evaluation, directly subordinated to the ministry. NEEC is in charge of preparing the evaluation material, polls on efficiency of the

education act, coordination on manuals, preparation of reports and analysis on national and international evaluations, organise the results management and train the expert evaluators. The values of NEEC are flexibility, transparency, objectivity, legality, cooperation, coherence, efficiency and public responsibility.

I presented the model from the Ministry of Education as a possible pattern to be followed in the Ministry of Defence as well. In chapter 2 it is presented the current situation, where the Land Forces Command (Army HQ) nominates, in the same time, the evaluated unit and the evaluation team. This situation can create conflict situation, especially when an evaluator is in direct professional relation with the evaluated unit. In one particular situation, the medical evaluator, staff officer in the Brigade HQ, had to evaluate the Battalion physician, who has already applied to be transferred as Medical Branch head in the respective Brigade. That meant the evaluated officer was in the course of becoming the evaluator's chief, and subsequently, the evaluator let the entire leniency to affect his professionalism. The reason of such situation (corrected on the spot, after being revealed), was the lack of qualified personnel.

In our opinion, the solution for such difficulties may be to keep the evaluation issues in a "separate basket". Having, at the CHOD[9] level, a designated structure in charge of evaluation of all services forces would grant objectivity, professionalism and permanent availability. The proposed model is presented in Figure 2 below.

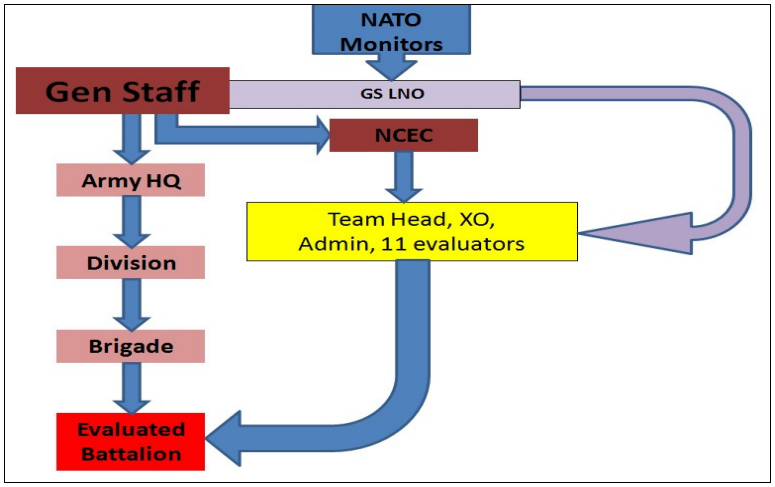


Figure no. 2. Proposed separation of the National Combat Evaluation Centre and evaluated unit hierarchy.

The whole spirit is the separation of evaluation players (teams, specialists, liaison officers, training staff and lessons learned implementation and integration) in one independent body, reporting directly to the Chief of General Staff (CHOD). Semantically speaking, the accreditation is about the person or organization entrusted to represent a certain competency of the originator. The central element of the accreditation is the confidence that the trustee will follow the prescribed procedure in the designated professional manner. Similarly, such an entity may represent the Ministry of National Defence, in the combat evaluation field, affirming itself as the competent independent body in charge of the evaluation leadership management. We consider that a National Combat Evaluation Centre (NCEC) may be founded on the ministry of defence order, in one of the three possible scenarios: under the direct subordination of General Staff Command (subordinated to the CHOD), organic to the Control and Inspection Corps (CIC), or directly subordinated to the ministry of defence. In the

[9] Chief of Defense, in accordance with AAP-006, NATO Terms and Definitions, Edition 2009.

case of positioning of such centre within the General Staff, there is the risk of competencies duplication, because, amongst the duties of the General Staff is also "the training and evaluation of headquarters and forces"[10]. In accordance with this point of view, we consider that the NCEC shall be positioned in the direct subordination of the CHOD. Another solution may be the NCEC positioned within the CIC, due to the similarity of duties and objectives. We consider that having this structure directly subordinated to the ministry of defence can be only a contingency solution, because an evaluation centre shall be connected to the military leadership realities. Concluding, we consider that the NCEC most efficient place is under the CHOD, similarly to the main services of the military, benefitting y the interaction of the systems under different command modules. Currently, the component in charge of standardised training influences the grade of the training audience, because in most of the cases, the trainer is also the only evaluator or one of the evaluation committee.

The figure 3 below considers the combat readiness evaluation just one component of the evaluation centre, together with maritime and air force evaluation components, a joint component and an administrative one.

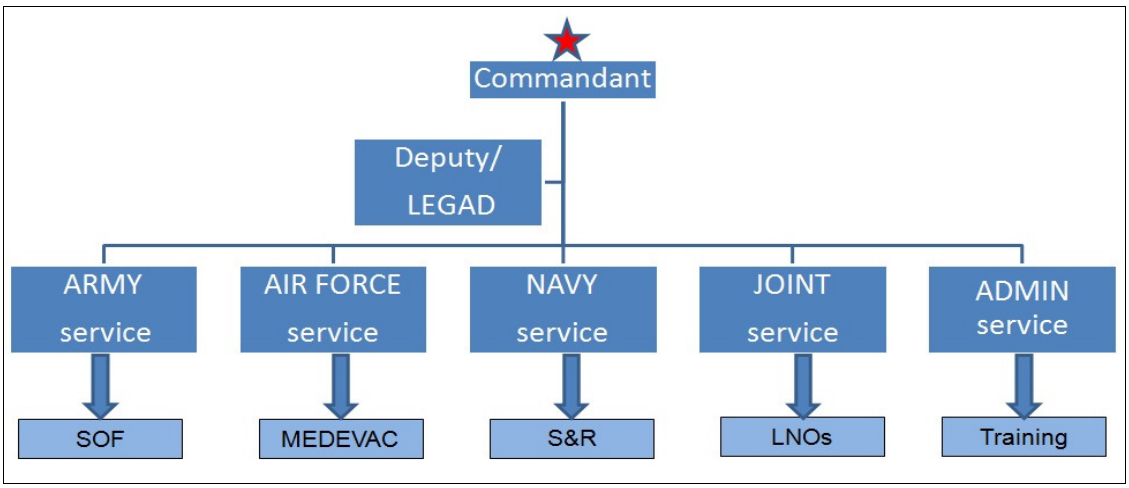


Figure no. 3. Proposed National Combat Evaluation Centre structure and additional functions.

Each of the components shall direct all activities from its own area of expertise, and each component shall also direct at least one additional smaller duty, from the common operational picture, such as special operation forces, medical evacuation, search and rescue, liaison with NATO entities, and last but not least, the training component. Each of the centre's components shall be manned with appropriate personnel, allowing the evaluation team frame for each service, and enough common specialists (as legal, CIS, CBRN, EOD, medical) to man two evaluation teams in the same time. The reason is that the NCEC shall be able to staff two different service evaluation teams, or one headquarters evaluation team, in order to save the human resources and to ensure a regular workflow in support of the national military. That is why, ideally, the evaluators part of these services shall possess at least a secondary qualification (such as armour and legal). Obviously, the NCEC will be in charge, primarily, of evaluation of units offered to the international organizations where Romania has commitments, such as NATO, UN or EU.

The accreditation process has, as final result, the certification of subject structure, granting that the examined body has the resources, expertise and specific standard operation procedures and instructions for the implementation of combat evaluation responsibilities.

[10] In accordance with site http://www.mapn.ro/smg/index.php, accessed on 26th of August, 2014.

More precisely, in the case of NCEC, the accreditation has to be performed by qualified structure from the General Staff, which will analyse the centre capacity on evaluation leadership, based on NATO relevant documents, and national regulations, harmonised with the alliance ones. During the accreditation process it shall be evaluated, also, the ability of NCEC in coordination with designated bodies from NATO command structure, as well as national ones within General Staff, because every two years the evaluation procedures are reconsidered, based on the lessons learned collected in the process.

4. The Functionality of National Combat Evaluation Centre

The main duties of the NCEC shall be the manning and management of the mobile evaluation teams that will address the evaluated units in their barracks. The evaluated units will consist, mainly, of the forces earmarked as national contribution to the NATO Response Force, or other international commitments. In its quality of national evaluation centre, the NCEC shall also manage the documents (manuals, instructions and general rules) pertaining the services evaluation field. The centre shall also assume the duties of national evaluation point of contact connected with NATO entities, in order to exchange functional information and improving the national military standards. The same cooperation is needed for the technical agreements required for the affirming the NCEC as a regional authority in charge of evaluation courses. This may involve periodic exchanges of trainers and evaluators, for the common benefit of NATO and MoND[11]. The evaluation courses (CREVAL for land forces, MAREVAL for maritime forces and OPEVAL for air forces) shall be designated, in our opinion, for the Romanian militaries, but also for the NATO and PfP nations within the geographical proximity. The course, being taught in English, would facilitate the international cooperation between Romanian and NATO/PfP soldiers, with added value for the future mutual understanding of the allied and partner nations in the abroad operations theatres. On the other side, Romania may have an additional opportunity to affirm itself as a regional authority in military education, through the partnership with NATO School Oberammergau[12] and the armed forces from our proximity, as Bulgaria, Hungary, Greece, the former Yugoslav Republic of Macedonia[13], Republic of Moldova, Turkey, Ukraine, Georgia and Armenia.

Conclusions

This article introduces a number of practical personal considerations about the implementation of a new structure, which may address the combat readiness evaluation process in a new design, completely compatible with the NATO policies. The proposal aims on objectivity, pragmatism, rationalization and efficiency, with certain potential of reaffirming Romania's role as a regional military authority, not only in the area of combat forces, but also in the field of military concepts and theories, in close connection with the *Smart Defence* and *Capabilities Targets* concepts. Finally, the material is offered as a starting point for the decision makers for a possible consideration regarding the national military evaluation process.

[11] Ministry of National Defence
[12] https://www.natoschool.nato.int/
[13] Turkey recognizes the Republic of Macedonia with its constitutional name.

Acknowledgement:

This work was possible with the financial support of the Sectoral Operational Programme for Human Resources Development 2007-2013, co-financed by the European Social Fund, under the project number POSDRU/159/1.5/S/138822 with the title ***"Transnational network of integrated management of intelligent doctoral and postdoctoral research in the fields of Military Science, Security and Intelligence, Public order and National Security – Continuous formation programme for elite researchers - "SmartSPODAS"."***

BIBLIOGRAPHY:

1. www.mapn.ro
2. www.edu.ro
3. www.nato.int
4. www.natoschool.nato.int
5. GANEA Jan-Florin, *Oppinions on Combat Readiness Evaluation Efficiency in Romanian Land Forces,* in Proceedings of the 9th International Conference "Strategies XXI", National Defence University "Carol I", 18-19 April 2013, Bucharest, ISSN 2285-8415.
6. AAP-06, NATO Terms and Definitions, Edition 2009.

INTERAGENTIES COOPERATION IN BIOLOGICAL ATACK IN ROMANIA

Viorel ORDEANU
Colonel (ret.) Senior researcher I, MD, PhD, Military Medical Research Center; Assoc. prof., University of Medicine and Pharmacy "Carol Davila", Bucharest, Romania

Marius NECSULESCU
Senior researcher I, MVD, PhD, Military Medical Research Center, Bucharest, Romania

Lucia IONESCU
Spec. biologist, Senior researcher III, Military Medical Research Center; PhD scandidate University of Bucharest, Romania

Abstract: *The prevention of the biological war is accomplished by the implementation of the Biological and Toxin Weapons Convention (BTWC, Geneva, 1972) which was signed by over 150 countries (including Romania) and by the international control of biological weapons and biological agents.*

Defence against bioterrorist attacks involves in addition the complex intervention of the National Health System, of the National Defence System, of the local communities, of the NGOs etc. The removal of the effects of the bioterrorist attacks is also of the competence of the Prefect's Office (with the specialized county bodies: the Territorial Civil Defence, the Public Health Authority, sanitary units, laboratories etc.), NGOs (e.g.: the Red Cross), but also to local communities.

The prevention of bioterrorist attacks is mainly a political and social problem, which is carried out firstly through the intervention of the secret services, of the police and of the justice system

Keywords: *biological attack, biological agents, CIMIC, medical protection, Romania.*

1. Defence against the biological attack

1.1. The prevention

The prevention of the biological war is accomplished by the implementation of the Biological and Toxin Weapons Convention (BTWC, Geneva, 1972) which was signed by 150 countries (including Romania) and by the international control over biological weapons and over biological agents.

The military use of biological weapons may be considered inefficient from the tactic and operational point of view; it is difficult from the tactic point of view and perilous from the strategic point of view (because an epidemic may escape control). Recent events show that the risk of bioterrorist attacks committed by civilians is higher than ever.

The fight against bioterrorist attacks involves in addition the intervention of the National Health System, of the National Defence System, of the local communities, of the NGOs etc.

The removal of the effects of the bioterrorist attacks is also of the competence of the Prefect's Office (with the specialized county bodies: the Territorial Civil Defence, the Public Health Authority, sanitary units, laboratories etc.), NGOs (e.g.: the Red Cross), but also to local communities.

The prevention of bioterrorist attacks is mainly a political and social problem, which is carried out firstly through the intervention of the secret services, of the police and of the justice system.

1.2. The fight against biological weapons

Biological crisis: major epidemiological emergency, with infectious etiology, which by the severity of the cases in humans/animals/plants or the great number of cases, leads to the disturbance of the social and economic life of a community. *Biological weapon*: system of unconventional mass destruction weapons, the ammunition of which transports biological agents and contaminate the enemy with the purpose of inducing illness. *Biological agent:* micro-organisms and/or microbial animal or vegetal toxins, used as specific ammunition in biological weapons, or used by terrorists in *"bio-chem"* attacks.

The management of the biological crisis

On a local, national or regional level, a virtual network for the Management or the effects of the biological attack, in which the first link and the most important link for public health is the general practitioner (personal doctor, institution doctor, military unit doctor), the first who comes into contact with patients, applies the first medical measures and alerts the competent authorities.

1.3. Institutions responsible with the intervention:

The Presidency orders in need the state of emergency or necessity, related to the intervention in the biological crisis.

The Parliament elaborates and/or amends laws which have an impact on the prevention and on the intervention in biological crises.

The Government takes concrete action for the intervention in the biological crisis by *the ministries, agencies and others:*

- the Ministry of Health (M.S.P.) with the Department for Public Health, the National Institute Cantacuzino, the Public Health Institutes, the Virology Institute, the Public Health County Authorities, the medical institutions of the country,
- the Internal Affairs Ministry (M.A.I.) with the Civil Defence, the Police, the Gendarmerie, the Fire Brigade, the Border Police, the Medical Direction etc.
- the Ministry of National Defence (M.Ap.N.) with the CBRN protection units (nuclear, biological and chemical), the Medical Direction, the Military Police, Special Forces etc.
- the Ministry of the Agriculture (M.A.A.) with the Veterinary Direction, the Agricultural Direction, the National Sanitary-Veterinary Agency, the Institute for Diagnosis and Animal Health, I.N.M.V. Pasteur, the County Veterinarian Directions, the veterinary institutions of the territory,
- the Ministry of the Environment (M.M.) with the County Environment Inspectorates,
- the Ministry of Transportation (the Sanitary Directions),
- the Ministry of Economy and of Finance (state business enterprises and the financing of activities).

The role and the position of the secret services

Independent secret services provide specific information:

- the Romanian Intelligence Service (S.R.I.), which, according to the law, coordinates antiterrorist action,
- the Protection and Guard Service (S.P.P.), which ensures the protection of officials,
- the External Intelligence Service (S.I.E.), which collaborates with foreign intelligence services,

Departmental secret services provide hierarchy intelligence and collaborate within the intelligence Community

Other components

Religious cults: The Romanian Orthodox Church and the other recognized cults.

Business enterprises: manufacturers and service providers.

NGOs: the Red Cross, Humanitarian organizations, Trade organizations, Trade unions.

Local communities: Prefect's offices, Mayor's offices, Town councils.

Citizens/population.

International collaboration: U.N, N.A.T.O., E.U., W.H.O. The Constitution of the E.U. also provides a solidarity clause:"E.U. shall mobilize all the instruments at its disposal, including military resources, in the case in which a member state is the victim of a terrorist attack or of a natural disaster", therefore, including in the case of a bioterrorist attack.

1.4. Responsibilities

The responsibility of coordinating counterterrorist actions belongs to:

- the government of the country which holds the presidency of the E.U. (by rotation every 6 months),
- the government of the attacked country/countries,
- the European Centre of Communicable Diseases (ECCD) which operates in Sweden since
- 2005, as an equivalent of CDC Atlanta from the U.S.A.

2. Present possibilities

2.1. The specific capacities of the Medical Direction of the Ministry of National Defence

The specific capacities of the Medical Direction of the Ministry of National Defence are important for the medical protection against mass destruction weapons (WMD) and especially for the combat against biological attacks, but the present level is very much reduced. It should permanently have at its disposal the necessary forces and the means for the medical protection against WMD with chemical, biological, radio, nuclear and/or explosive agents (CBRNE): the diagnosis, the prophylaxis, the treatment and the recovery of the injured, through military sanitary units.

Sanitary military units involved:

- the Central Military Clinical Emergency Hospital "Carol Davila" Bucharest,
- the territorial Military Emergency Hospitals (x 11),
- the ROL 2 Military campaign Emergency Hospitals (surgical or specialized), which become active on call,
- Medical Diagnosis and Treatment Centres (polyclinics),
- Military Medical Research Center,
- the Preventive Medicine Centre,
- the Transfusional Haematology Centre,
- Sanitary storage facilities,
- Medical-military education institutions.

Focus: The main institution specialized in the elaboration of the methods and of the means for medical protection against CBRN agents is the Military Medical Research Centre (CCSMM), Bucharest, also against bioterrorism.

2.2. Specific existent capacities

CCSMM is equipped with specialized laboratories, including a Laboratory for Medical Anti-infectious Protection and for Epidemiologic Emergencies, which operates since 1968 as a specific unit for medical protection against biological weapons. It conducts fundamental medical research in the field of microbiology and of epidemiology, through interdisciplinary research teams: bacteriology, Virology, mycology, toxinology, anti-infectious pharmacology, zooanthroponoses, molecular biology, genetics, identification of biological agents etc.

Diagnosis

For the microbiological diagnosis, the laboratory owns:

- adequate space;
- qualified personnel (but which was reduced to a critical level during the last few years);
- appropriate equipment (fixed assets, inventory, consumables, biobasis, computer technology etc.);
- appropriate facilities;
- standard operating procedures (POS) according to the directions of the Ministry of Health (according to the WHO and EU recommendations) and there is the intention to comply with NATO standards as well.

Equipment:

- MALDI TOF mass spectrometer LT 20 Microflex Bruker
- MiniApi computer system
- PCR Line and a sequencer for the electrophoresis of nucleic acids (which was used for the first identification of the H5N1 virus of the avian influenza in Romania, in 2005)
- ELISA Tecan computer system
- TLC Line chromatography with computerized densitometry
- Optical computer microscope, with image processing
- Electrophoresis line with computerized densitometry
- Microbiological biosafety extractor hoods: class III, II, I laminar flow hoods, "glove box" extractor hood with controlled atmosphere etc.

2.3. Biological agent diagnosis.

For crisis situations**,** the lab has a P2+ level laboratory for the Diagnosis of Biological Agents, which inclusively performs survey reports for mail and for objects suspected to be biological weapons or are contaminated with biological agents, at the request of military units. This Laboratory was formed according to the Order of the SMG (General Staff of the Ministry of National Defence), in 2001 and put into operation in 2002, as a consequence of the bioterrorist attacks from the U.S.A. and from the E.U. The facility was put into operation by reorganization: conception, space, personnel, equipment.

The mobile intervention unit

In 2002, at the Order of the S.M.G. (General Staff of the Ministry of Defence), The Mobile Biological Intervention Unit (EMI-Bio) was formed and put into operation in 2003, consisting of a main team and a backup team, NBC and medical protection equipment, specific intervention materials for the collection of samples and for the transportation of the samples to the laboratory and a minimum of field diagnosis means. Starting with 2005 this structure is included in the system for NBC Supervision of the Romanian Army and it permanently has at its disposal a military transportation helicopter.

The anti-epidemic reserve

Since 2005, an Anti-epidemic reserve was formed for field intervention, in case of a biological crisis (diagnosis, prophylaxis, sanitary field research), with the unit's own means and forces, reserve which is constantly updated.

Since 2006, a micro production laboratory is operational for microbiology and epidemiology specific materials, for the unit's own use during interventions in situations of biological crisis, organized and equipped with the unit's own means and forces.

Special laboratories

Starting with 2007 we organized, in collaboration with SMG, the NBC Defence section, a Laboratory for the Detection and for the Identification of biological agents**,** with BSL 2+; its specific equipment may be transferred on request onto a vehicle in order to have a mobile laboratory in need, at the order of SMG.

There is a system of functional links with highly specialized laboratories in case of need.

The multi-annual medical-military scientific research plan of the CCSMM involves laboratories in top fields for the medical protection against CBRN / WMD agents and weapons.

2.4. Present concerns

The CCSMM took part in the national scientific research competitions organized each year by the Ministry of Education and of Research and won a state grant for the development of a Highly secure microbiology laboratory BSL 4 (maximum) and a complementary Level 3 secure bio base; these objectives are in progress.

After the fulfilment of the above-mentioned objectives, the laboratory becomes a specific facility, we are compatible with NATO and we can be a possible node of the CBRN/DSS supervision network.

Perspectives

The main of the medical military service in the fight against biological terrorism is to have the strictly necessary facilities for the diagnosis, the prophylaxis and for the specific treatment in biological attacks, at the present level, provided by STANAG (NATO), by the E.U. legislation, by WHO and by the national legislation, which complies with these. The epidemiological management of the effects of the biological attack requires a very good collaboration between all forces involved, especially military-civilians (an express requirement of NATO for CIMIC), but also on a national-international level.

Conclusions

The management of the effects of the biological attack requires a very good collaboration between all forces involved, especially military-civilians (an express requirement of NATO for CIMIC), but also on a national-international level. Although this subject is itself confidential, its principles and conception must be known by all main actors, in order to be put into practice when needed.

BIBLIOGRAPHY:

1. ORDEANU Viorel, NECSULESCU M., DUMITRESCU G. “Implicatii ale existentei unei echipe mobile de interventie biologica asupra securitatii militarilor” Revista de Stiinte Militare, editata de Sectia de Stiinte Militare a Academiei Oamenilor de Stiinta din Romania, (ISSN: 1582-7410) nr. 1 (24) 2014, pp. 53-59.

2. ORDEANU Viorel, IONESCU L., BICHERU S. “Statutul si rolul laboratorului biologic analitic dislocabil pentru aparare CBRN in teatrul de operatii” Revista de Stiinte Militare, editata de Sectia de Stiinte Militare a Academiei Oamenilor de Stiinta din Romania, (ISSN: 1582-7410) nr. 1 (24) 2014, pp. 60-69.
3. ORDEANU Viorel, POPESCU D., HERTZOG R. “Statusul imunitar postvaccinal la militarii dislocati in teatrele de operatii” Revista de Stiinte Militare, editata de Sectia de Stiinte Militare a Academiei Oamenilor de Stiinta din Romania, (ISSN: 1582-7410) nr. 1 (24) 2014, pp. 70-80.
4. ORDEANU Viorel, ANDRIES A.A., HINCU Lucian “Microbiologie si protectie medicala contra armelor biologice” Editura Universitara “Carol Davila” Bucuresti, 2008.

INTERNATIONAL POLICIES AND STRATEGIES ON CYBER SECURITY

Cătălin-Iulian BALOG
National security expert within Ministry of National Defence.
E-mail address: catalin.balog@gmail.com

Abstract*: A comparative analysis of a new generation of national cyber security strategies shows that cyber security policies have undergone a turning point. In many countries, this strategy has become a national priority and receives a strong support from the political leadership. The analysis of these strategies cannot be inferred a single definition of cyber security. Even so, all these strategies reveal tendencies of integration and inclusion. They are approaching on cyber security in a holistic manner, including issues related to social, educational, legal, diplomatic, economic, technical, and military force structures and even intelligence structures areas. In this context, the assessments on the concept of sovereignty have become increasingly important.*

Keywords: *cyber space, security, strategies, critical infrastructures, vulnerabilities, threats, risks.*

1. Cyber security

1.1. A new generation of security policies

This paper examines the emergence of a new generation of government policies, called cyber security strategies, for 10 countries, covering similarities and differences, identifying significant changes from previous strategies and the new generation.

The new generation of national cyber strategies aims to ensure a path to economic and social prosperity and to protect a society dependent on cyber space against specific threats. A key challenge in the current cyber security policies are the simultaneous achievement of these two objectives and at the same time maintaining the openness of the Internet as a platform for development of innovation and a source of economic growth and social prosperity.

Analyzed cyber security strategies assume that economy, society and governments rely on the Internet to conduct essential functions and cyber threats are growing and evolving at a rapid pace. The goal of most strategies is to extend government efforts at political and operational coordination and clarification of roles and responsibilities of the bodies involved. They emphasize the need for cooperation between the public and private sectors and also the need to respect fundamental values such as freedom of expression and freedom of information and privacy. However, they call for better international cooperation; some exhibits flexible approach and emphasizes the economic dimension of cyber security policy, other creates multilateral dialogue conditions for the development of cyber security policies and implementation of the common processes.

Action plans reinforce key priority areas identified in the early 2000s, focusing on some activities like research and development on cyber security and real time monitoring of governmental infrastructure. Action plans aim is to provide the conditions for economic development of cyber security as a robust industry. They identify partners and business areas as economic development opportunities in the field of cyber security. Also establish partnerships with ISPs and encourage deployment of attack and defense exercises in cyber space.

It can be appreciated that security strategies developed so far are still in its infancy and it will take time for them to reach the stage of maturity. However, a key challenge for governments is that they must be prepared to deal with a possible complex cyber incident as required by virtually all strategies analyzed, in a way that does not prejudice the openness of the Internet, which is essential for the vitality of the Internet based economy.

1.2. Cyber security as a political priority

The analysis of new generation of national cyber security strategies reveals a significant evolution in government policy development, brought by the government priorities on cyber security.

According to these strategies, the overall governments assessment is that:

• Internet, information and communications technology (ICT) are essential for economic and social development and form a critical infrastructure. In a general context of economic downturn, an open Internet and ICT are a new source of growth and innovation, of social welfare and individual expression. As the Internet economy grows, the whole economy and society, including governments are increasingly becoming dependent on the digital infrastructure to perform the essential functions.

• Threats evolve and multiply at a rapid pace. They are still initiated by criminals, but there are new sources such as other states and political groups who may have other motivations than money purchase, such as certain types of "hacktivism" (Anonymous) destabilizing actions (eg. Estonia, 2007), cyber espionage, cyber sabotage (eg. Stuxnet, 2010) and even military operations. Individuals or malicious entities are better organized, especially to conceal the traces, and the complexity has increased significantly, showing clear signs of professionalism.

As a consequence, the goal of most new cyber security strategies has evolved to protect users and businesses, as separate physical entities, to protect society as a whole. This change results from the changing role that the Internet plays in the society. When the Internet was just a useful platform for users and businesses, the consequences of failures were managed at the level of each user or enterprise, and government policy has sought to provide support to prevent and manage these incidents. As the Internet has become essential for the economy and society, the consequences of failure can have a direct impact on society, as a whole. So, the aim of cyber security strategies is designed to achieve two interrelated objectives: • to strengthen cyber security for Internet economy to ensure the path to economic and social prosperity • protection of society dependent on cyber space against cyber threats. A key challenge in the current cyber security policies is the simultaneous achievement of these two objectives and at the same time maintaining the fundamental values and the openness of Internet.

From the perspective of a modern economy, Internet criticism lies in the consequences of cyber security policies development, mainly being about adopting those strategies that address cyber security in an integrated and comprehensive manner. Governments recognize the need to address all aspects of cyber security in a holistic manner, rather than a piecemeal, as in the past. The new cyber strategies are brought to the government's priorities, including issues related to the social, educational, legal, diplomatic, economic, technical, and military force structures and even structures of intelligence. In most cases, this integrated approach is supported by a strong leadership, at the level of head of state or government, illustrating the importance of cyber security concerns regarding the government's priorities.

Not all strategies using the terms "cyber space" and "cyber security" and definitions vary from state to state. Most states include the concept of critical information infrastructures in their strategy.

2. Common strategic concepts and action plans

2.1. Common strategic concepts

Most national cyber security strategies share the following concepts:

• *Expanding government coordination at the political and operational level.* Given that cyber security is a matter of national priority, responsibility for cyber security policies and their implementation lies clearly to the government. However, no agency can not claim that it has sufficient authority to manage all aspects of cyber security. The coordination between the bodies is essential. The responsibility for coordination of these bodies lies generally to an existing agency or one newly established, and responsibilities of other government bodies involved are also assigned clearly aiming at facilitating cooperation, avoid duplication and stimulate initiatives. This evolution from a multi-organizational approach to an inter-organizational approach requires a strong leadership to allow the coordination and cooperation in a format of the existing government. Provisions and specific protocols differ from one state to another and reflect the culture and style of governance.

• *Strengthen of the public-private cooperation.* All strategies recognize that cyber space is largely owned and operated by the private sector and users play a key role. They recognize that policies should be based on partnerships, including public-private partnerships that may include Internet, civil society, academia, business communities and professional communities. However, the modalities of such consultations and the level of detail provided in these strategies differ.

• *Improving the international cooperation.* International cooperation and the need for better alliances or strategic partnerships with other countries and allies, including facilitating the development of capacities in the less developed countries are key objectives shared by most strategies. However, most states offer few details on how to conduct extensive international cooperation. Exceptions include the United States, which has developed an international strategy for cyber space and the United Kingdom, who initiated an international dialogue through the London Conference on cyber space, in 2011, and promoted the concept of international norms of cyber space, which was taken by the strategies of Australia and Germany. The need for greater harmonization of legislation against cyber crime is often mentioned generally in support of the Budapest Convention, in 2001, relating to cyber crime. International and regional organizations such as Council of Europe, European Union (EU), Group of 8 (G8), Internet Governance Forum (IGF), Organization for Economic Cooperation and Development (OECD), Organization for Security and Cooperation in Europe (OSCE) and United Nations (UN), including International Telecommunication Union (ITU) are mentioned, but without much detail regarding their role. The exception is the North Atlantic Treaty Organization (NATO), mentioned in the security strategies of some countries about cyber security in the military context.

• *Respect for fundamental values.* All strategies emphasizes the need for cyber security policies to respect fundamental values: privacy, freedom of expression and freedom of information. Several strategies explicitly mention the need to keep the Internet open and no strategy proposes mitigating the openness of the Internet in favor of enhanced cyber security. Instead, an opened Internet is generally described as a condition for the development of the Internet economy further.

2.2. Emerging strategic concepts

The analysis of national cyber security strategies allow identification of key concepts that are not necessarily expressed by all states, but indicate possible new trend. The most strategies place particular emphasis on the following:

• Considerations on the *concept of sovereignty* in the cyber security policy; for example, national and international security, intelligence, military and defense issues.

This development is a direct consequence of the finding that cyber security deals with the protection of society as a whole and requires an integrated governmental approach . Considerations on the concept of sovereignty occur in the *domestic policy*: i) at the strategic level, for example, by recognizing cyber threats targeting the military or risk of cyber espionage from other countries, ii) at the organizational level, the relationship between departments and ministries of foreign affairs, national defense and intelligence structures – included in the inter-governmental policy making – with a body of national security inter-organizational type, with responsibility for cyber security coordination, iii) at the operational level, for example through information structures that play key roles as sources of information and warning elements. Considerations on the concept of sovereignty also arise at the level of *foreign policy*: i) strategies mention the need for international dialogue about the "rules of engagement" or "confidence building measures" in cyber space, ii) strategies highlights the role of organizations such as NATO and the OSCE in addressing these issues, and iii) strategies mentioned operational cooperation between intelligence services, on the exchange of information between allies.

• *Flexible policy approach.* Internet economy is a dynamic environment in which technologies, markets and customs are constantly and unpredictably evolving in the benefit of economic growth and innovation, and in which threats are also constantly evolving. Some cyber policies promoting flexible strategies to maintain the openness of the Internet, but also factors that allow the Internet to generate economic and social benefits. Other strategies support policies that enable quick decisions and knowledgeable, incorporates rapid feedback mechanisms and cycles include effective learning and effective implementation of new measures. Some believes that self-regulation strategies should be favored, and the law should be considered only when self-regulation is not effective or is not possible.

• *The importance of the economics of cyber security.* While the goal of all cyber security strategies is to ensure cyber security, maintenance and development of social and economic prosperity through sustainable development and requires an active Internet visibility of the economics of cyber security. Some states argue that a higher level of cyber security will give their economy a competitive advantage. They recognize that economic factors play a key role in improving cyber security. Other strategies that leverage encourages flexible policies to stimulate the market and economic operators, encouraging the use of security labels on products and services. Several states have set as a priority the development of a cyber security industry. They also mention the possible development of a sector such as cyber security incidents. Some strategy identifies the need to reduce dependence on technology as a very important objective.

• *The benefits of multilateral cooperation.* Many strategies believes that public-private dialogue is essential for the development and implementation of good cyber security policy. However, specifying the details of government employment in such a dialogue are shallow or even no details on this. Some strategies assessed as good as setting up a dedicated body of public-private dialogue and indicate who may be parties who could provide information and advice to government. It is generally recognized that feedback came from businesses is an essential element, including the development and implementation of these strategies, but information about the consultation of civil society beyond academia, are minimal.

2.3. Expanded and consolidated action plans

In general, cyber security strategies include or be accompanied by the adoption of action plans designed to strengthen key areas, as follows:

• *security of the governance*: action plans include a variety of initiatives, from developing a body of warning to the organization and management of government infrastructure and development of public sector audits;

• *protection of critical cyber infrastructure*: in general, action plans include measures relating to the protection of critical cyber infrastructure;

• *fight against cyber crime*: action plans include initiatives to develop law enforcement bodies and improving the legal framework on cyber crime and promote international cooperation under the Budapest Convention (2001);

• *increase warning*: include action plans several initiatives aimed at specific segments of the population (minors) and society (small and medium enterprises, government decision makers and critical infrastructures);

• *education and training*: action plans recognize the need for highly qualified workforce in the cyber space. Developing skills in cyber security is identified as a priority in many countries;

• *quick response*: action plans recognize the role of CERT or CSIRT teams and support the development or strengthening their national.

Research and development granted a relatively low level of attention, before developing these strategies, receive a great attention in the new cyber security strategies, generally focusing on a better organization and coordination of existing efforts on research and development of cyber security in public-private partnership. In this context, it should be noted that only the United States has adopted a strategic plan for research and development in cyber security at the national level.

Some cyber strategies introduce new topics in action plans such as:

• development of some real time warning and monitoring situation capacities, especially for critical infrastructure of the government;

• development of some policies to support a cyber security industry, more robust;

• consideration of some specific business and actors without a strict definition of the critical cyber infrastructure could cause significant damage to the economy;

• development of some partnerships with Internet service providers (ISP) to thwart botnet threats, including customer participation;

• identification of factors and economic incentives, such as conditions of security breach notification rules concerning access to confidential data or security labeling on products and services;

• execution of cyber security exercises (defense and attack), including across borders;

• development of rules and principles for digital identification;

• development of policies to protect children in cyber space.

3. Assessments and conclusions

3.1. Considerations of non-governmental organizations

In general, non-governmental organizations concerned agrees to the following: i) cooperation and multilateral cooperation are the best means to develop effective cyber policies that respect the global, open and interoperable Internet; ii) options expressed through policies must be flexible enough to adapt to the dynamic nature of the Internet; iii) there are required more robust cyber security policies based on evidence, something that generally is not covered by cyber security strategies.

Non-governmental bodies consider that the gap between the concept of *sovereignty* and *cyber security* policies is increasingly blurred and that this trend could have unintended consequences. For example, the business community stresses that could face additional charges, while civil society is concerned that its advisory role could be reduced, which could

affect the transparency of the decision. There is also concern that the aggressive rhetoric could take place of the debate on cyber security policy, with the risk of economic and social benefits decreasing due to the openness of the Internet.

In addition, given the improving consultation with interested non-governmental organizations, civil society proposes several measures to ensure that cyber security policy development remains a transparent process. For example, cyber security strategies could include a sunset clause to prevent measures that were legitimate at the time of their adoption, jeopardizing fundamental rights as technology evolves. Policy initiatives could include a systematic risk assessment, with details of prejudice that they could produce, and an assessment of their impact on fundamental rights such as privacy, freedom of expression and freedom of information.

A number of other proposals are submitted by non-governmental organizations concerned *to enhance the effectiveness of cyber security strategies*. For example:

• Consistency of measures provided for cyber security strategies with other similar initiatives could be evaluated systematically by the civil society. For example, laws that criminalize the actions of "hacking" could take into account that in this case the legitimate research could use the same techniques.

• Governments, as owners and operators of computer networks and communication systems may be an example by adopting the best practices, technologies and developing legislative requirements. The respect of confidentiality, the existence of appropriate and best practices can provide a clear direction for the business. Finally, it is estimated that some government technologies could be made available to the entire society.

• Policy makers may seek advice from the professional communities in developing security policies as early as possible to avoid some wrong decisions in terms of technical or technological.

• Security policies could encourage the development of open standards to enable innovation, security solutions and avoiding government imposed unilateral modification of standards, taking into account the experience of professional groups specializing in the development of open standards.

• Collecting the empirical evidence could be encouraged to better assess the relevance of security strategies and policies and to support risk-based approach, referred to as priority in cyber security strategies. There were highlighted various means to encourage evidence-based policy making to counteract the distrust that many users or entities manifest in the provision of information on cyber incidents in which they were part. These include harmonization mechanisms for reporting incidents and inform the society about the risks which government systems and critical cyber infrastructure are facing.

Finally, the *international dimension* of cyber security policy is highlighted by the business and technical community. They emphasize that the requirements imposed by some countries to ICT equipment generates complex challenges for economic development. It emphasizes that technical barriers in trade, for example in the form of requirements imposed by local standards, redundant security certification schemes or interference in the value chain have the effect of increasing default costs, limiting functionality, innovation and ultimately reduce deformation conditions of competition. They require government policies to allow implementation of comprehensive industrial and efficient solutions, for example by adopting open international standards, recognition of cross conditionalities and increase of warning level of the less developed countries.

3.2. Conclusions

The emergence of the considerations on concept of sovereignty in cyber security strategies are likely to influence the evolving security policy on the long term. At this stage,

the considerations on concept of sovereignty are separated from economic and social aspects of cyber security, but the common parts are visible. For example, in some cases, policy coordination is charged of some bodies whose mission focuses on issues of sovereignty; some strategy states that technological facilities involve side effects that can manifest in many different places: from the intelligence community to the cyber security industry; based on these considerations on the concept of sovereignty, new suppliers of products and services that benefit from investments in the research and development industry are emerging on cyber security market; and finally, in some countries, the intelligence community and armed forces become important providers of jobs in cyber security. Understanding og the implications of "cross-fertilization", on the short, medium and long term may become increasingly relevant to the cyber security policy develepment proces.

Establishment of some governmental coordination points through national strategies, creates an opportunity to strengthen international cooperation both at policy and operational levels. Each member state may consider extending these coordination efforts by the designation of a international *contact point* (Point of Contact, POC) at the governmental level, available, for example, to facilitate the distribution of external requests for information on the actions of cyber space or internal bodies with responsibilities in the field or at the level of policy or operational or emergency, informational or otherwise.

Although cyber critical infrastructure protection is generally included in the scope of strategies, the *problem-border interdependence* is rarely addressed at the strategic level. Further cooperation in this area is certainly a mutual interest.

Just out of respect it can say that cyber security policy seems to have reached a level of maturity compared to previous generations, developed and implemented since 2000. This new generation really enjoy a strong leadership and visibility under government programs, better coordination and greater involvement of all interested bodies. But at the same time, we should mention that the policy challenges are multiplying, which suggests that governments face *another level of complexity*. For example, governments must respond simultaneously to • the need for better coordination between the organizations involved, with a greater degree of centralization, and to • the need to boost the decision-making process – almost in real time – at all levels. Another major challenge is the need for a holistic approach that takes into account the considerations of sovereignty and socio-economic concerns, the involvement of a wider range of government agencies and increasing cooperation with the private sector. Another challenge is the need to preserve the openness of the Internet and basic values.

Finally, the lack of details on the measures, lack of metrics and methodologies for evaluating the effectiveness of these measures, but the fast pace adopted by some states to review new policies and strategies, among other factors, suggests that this new generation of cyber security strategies is still at an early stage.

Refining and implementing current policy packages will require time. But at the same time, a key challenge for governments is the need to be prepared to face serious cyber incidents, such as is provided in almost all strategies in a way that does not affect the openness of the Internet. Taking into account that cyber security policies grows continuously and permanently, a key question will be whether and how the governments of these countries will ensure the openness of the Internet, as part of cyber security strategies.

Acknowledgement:

This work was possible with the financial support of the Sectoral Operational Programme for Human Resources Development 2007-2013, co-financed by the European Social Fund, under the project number POSDRU/159/1.5/S/138822 with the title ***"Transnational network of integrated management of intelligent doctoral and postdoctoral***

research in the fields of Military Science, Security and Intelligence, Public order and National Security – Continuous formation programme for elite researchers - "SmartSPODAS"."

BIBLIOGRAPHY:

1. *** *„Strategia de Securitate Cibernetică a României"* şi *„Planul de acţiune la nivel naţional privind implementarea Sistemului Naţional de Securitate Cibernetică"* (în M.O. nr. 296 din 23 mai 2013, H.G. nr. 271/2013).
2. *** CERT, *Governing for Enterprise Security*, http://www.cert.org/governance/
3. *** FFIEC, *Handbook Definition of Reputation Risk*, http://ithandbook.ffiec.gov/it-booklets/retail-payment-systems/retail-payment-systems-riskmanagement/reputation-risk.aspx.
4. *** http://news.bbc.co.uk/2/hi/technology/6653119.stm
5. *** http://www.securitatea-informatiilor.ro
6. *** http://www.sri.ro
7. *** NATO, Cooperative Cyber Defence – Centre of Excellence, *National Strategies & Policies,* https://ccdcoe.org/328.html.
8. *** NCSA, *What Businesses can do to help with cyber security*, http://www.staysafeonline.org/sites/default/files/resource_documents/What%20Businesses%20Can%20Do%202011%20Final_0.pdf.
9. *** US-CERT, *Socializing Securely: Using Social Networking Services*, http://www.us-cert.gov/reading_room/safe_social_networking.pdf.
10. *** US-CERT, *US-CERT's Protect Your Workplace Posters & Brochure*, http://www.us-cert.gov/reading_room/distributable.html.
11. DUNNIGAN James F., *Noua ameninţare mondială: cyber -terorismul*, Editura Curtea Veche Publishing, Bucureşti, 2010.
12. GORDON A. Lawrence, *Cyber security risk management: an economics perspective*, http://www.rhsmith.umd.edu/faculty/lgordon.
13. Marshall McLuhan, *Mass-media sau mediul invizibil*, Editura Nemira, Bucureşti, 1997
14. ROBINSON Neil, *Cyber security Strategies Raise Hopes of International Cooperation*, http://www.rand.org/pubs/periodicals/rand-review/issues/2013/summer/cyber security-strategies-raise-hopes-of-international-cooperation.html.

CRIME IN CYBERSPACE. APPROACHES ON LEGISLATIVE REGULATION IN THE FIELD OF CYBER CRIME

Dragoş Claudiu FULEA
Romanian Intelligence Service.
E-mail address: dfulea870@dcti.ro

Marius Ciprian CORBU
Romanian Intelligence Service.
E-mail address: mcorbu870@dcti.ro

Abstract*: In the absence of a universally accepted legal framework at the international stage, assuring individual rights and freedoms within cyberspace, the extended phenomenon of the online crime, including the cyber attacks is creating the premise of serious collateral effects, hardly to predict, as significant financial and material losses.*

Threats deriving from virtual space are borderless and, given the speed of propagation characteristic of the current stage of development of the Internet (WEB 2.0 platform), they can spread before the majority of users have the chance of an early warning. Even under the circumstance of an exististing, performant warning system only a small number of users have the time, expertise or technical means necessary to protect themselves.

The paper intends a brief overview of the current cyber security status, in the context of an alarming proliferation of threats launched, from cyberspace, by state or non-state actors.

Keywords: *Cyber attacks, digital threats, IT criminality, cyber crime.*

Introduction

In the last decade, in the literature concerning the topic of cybercrime frequently occur terms such as "computer crime", "high-technology crimes," "computer-related offenses," which are insufficiently clearly defined or agreed[1]. While some legal experts consider these offenses as part of a new category, the other assimilate it to traditional forms of crime amended by "classic" laws.

In fact, all these linguistic constructions betray a feverish concern, a coagulation of approaches in order to combat the phenomenon of crime in cyberspace, a process which is sped up under the stress of multitude cyber attacks launched by State actors or non-State entities.

Under the terms of an uptrend of crimes in cyberspace favored, in equal measure, by technological breaches and the vulnerabilities of human online interaction, the paper intends a brief presentation of the current security status, in the context of an alarming proliferation of threats from cyberspace in the absence of a uniform international legislation on cybercrime.

[1] The European Commission, *„Towards a general policy on the fight against cyber crime"*, COM(2007) 267.

1. Cyberspace insecurity

Within the virtual space, the information relating to any sequence of an Internet user's personal life, such as family circle and close relationships, preferences, personal interests, can be valorized by specialized personnel belonging to interested actors, similarly as achieving a puzzle, in order to draw a psychological profile, or to identify the main personality dominants.

On the other hand, cybercriminals use the offensive, social engineering methods for purposes of exploitation of the human vulnerabilities[2] such as sexual attraction, greed (offer of "bargains"), vanity (the belief that the victim was chosen from millions of users), credulity (attacker claims is a major corporation), convenience (the abuser bets on the indifference of the receiver to verify the identity an unknown issuer), compassion (dramatic humanitarian support request) and urgency (immediate need for humanitarian aid).

It is to be mentioned that works assessed by prestigious practitioners[3] highlight the following six categories of offenders:

- Hackers – especially young people who breach the computer systems driven by motivations, especially related to intellectual challenge, or in order to obtain and maintain a particular status in the hacker global community;
- Spies – persons who enter into computer systems to obtain intelligence, according to specific orders of state or non-state actors;
- Terrorists – people who enter into computer systems in order to produce fear, for political purposes or those affiliated to the activist movement;
- Economic perpetrators – attackers entering the computer systems of competitors, with the aim of obtaining financial gains;
- Professional criminals – perpetrators entering the computer systems in order to obtain personal financial gain;
- Vandals – persons that are entering the computer systems just for the purpose of creating extensive damage, destroying valuable data.

In this context, it should be emphasized that an attack does not appear out of the blue, from nowhere, as a magician's "rabbit out of the hat" trick, but is a logical sequence of effects, stages and consequences initiated and led by the offender.

In this sequence, one can find both the action directed towards a target and the use of an IT&C tool to exploit target's vulnerabilities. Also, one can find the criminal intention, whereas an attack aim to fulfill as a goal, an unauthorized result, viewed from the perspective of the user or the system administrator.

Broadly speaking, attacks are composed of a chronological succession of five logical steps to be taken by an intruder, as follows:

- Identifying the target and vulnerabilities exposed by her, deriving from the social communication within cyberspace;
- Using a IT&C tool to harness the easiest vulnerability in order to obtain an unauthorized result;
- Succeeding an unauthorized result, in order to collect and exploit data or intelligence belonging to the target;
- Securing an anonimized channel connecting the target to permanently or repeatedly exploit the mark;

---

[2] *Cisco 2013 Annual Security Report* accessed on 4 July 2014 at http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2012.pdf.

[3] John D. HOWARD, *An Analysis of Security Incidents on the Internet,* http://resources.sei.cmu.edu/asset_files/WhitePaper/1997_019_001_52455.pdf, accessed on 13 July 2014.

- Triggering, if necessary, an event or series of events on a target's computer to cover up - by destroying the data - the traces of the intrusion.

To trigger an attack of proportions with real, quantifiable, chances of success against the infrastructure of a target State are necessary important technological logistic and financial resources, but mostly human resources trained specifically for this purpose. At the same time, it is needed a centralized enhanced coordination of the attack. All these prerequisites are met mostly by a State actor or a non-State actor, even corporate, but featuring significant global capabilities.

In the early 2013, along with other allied NATO countries, Romania has undergone an unprecedented cyber attack ("Red October"). The operation was one of the most advanced and complex digital attack campaigns that aimed at gathering data held by government institutions and diplomatic missions, as well as of research institutions around the world. Attackers have created a malware attack all-in-one platform, which included more malicious files and extensions developed to rapidly adjust to different conformations and to gather data from compromised machines. The malware was designed to steal information even from mobile devices (such as Smartphones), network equipment (routers, switches), with the possibility of recovering deleted files.

Even as this paper is in progress, another cyber attack it is carried on against institutions from Eastern Europe and Asia (Romania is on the 9th place from top ten targets) by entities located on Russian Federation soil, in the setting of regional crisis caused by Moscow's involvement in the actions of undermining the sovereignty of Ukraine[4]. This time, the Russian so-called "hackers" are massively using a Trojan Virus called Kelihos.

From the legal perspective, the criminal phenomenon generated by the technological revolution within cyberspace clearly reveals two issues. The first relates to the inability of a State, no matter how technologically advanced, to handle alone threats originating from the virtual space. The second highlights the difficulty of implementation at national level, of a way for the application of legislative provisions within the defined territory jurisdictions, in the absence of a legislative framework on cyber crime, agreed at the international level.

2. International preoccupation on legislative regulation regarding the field of cyber crime

At the European Union level, the responsibility of improving the EU capabilities, the Member States and the business community in order to prevent and manage the challenges of cyber security rests with the European Network and Information Security Agency (ENISA).

In February 2003, the United States has adopted, for the first time, the national strategy for Cyberspace Security as part of a series of measures taken after the terrorist attacks of 11 September 2001. This document defines a set of priorities in ensuring American virtual space, including the establishment of a national response system to cyber threats and the setting of an early warning system.

In recent years, countries that have an economic infrastructure dependent on IT&C instruments have proceeded to complete their legal framework in the field of defense and national security by adopting different strategies relating to cyber security, which define the term "cyber-terrorism" and it ranks at the top of national security risks (United Kingdom – in June 2009 – "Safety, Security and Resilience in Cyberspace", Australia – in November 2009, Canada – in October 2010, The Netherlands – in July 2011 – "Success Through Cooperation", Germany – in March 2011, New Zealand – in June 2011).

[4] http://www.b1.ro/stiri/high-tech/bitdefender-avertizeaza-cu-privire-la-un-atac-cibernetic-care-indeamna-la-atacarea-site-urilor-guvernamentale-din-occident-care-au-impus-sanc-iuni-rusiei-90526.html, accessed on 7 September 2014.

At the NATO Summit in Bucharest in 2008, was raised for the first time in a formal framework, the cyber terrorism matter. The talks have resulted at operational and strategic level, by setting up the Cyber Defense Management Authority, which has the primary responsibility for coordinating cyber defense of the Alliance and the establishment at Tallinn, Estonia, of the Cooperative Cyber Defense Centre of Excellence, which is upgrading and developing strategies to specific IT&C threats.

NATO's Strategic Concept regards the cyber attacks as one of the main threats to the security of the Alliance. Cyberspace is considered as a global space and theater of military operations. Defining the virtual dimension as space of confrontation - beside the land, sea, air and extra-atmospheric space has implied a resizing of all threat response components (organizational, policies, budget and human resources). Subsequently, in June 2011, on the occasion of launching the Strategy for Operating in Cyberspace[5], by the U.S. Department of Defense, the cyber attacks on strategic infrastructure has been defined as "acts of war" that might generate a classical military response.

In addressing security risks from cyberspace, NATO co-operates with international organizations (UN and EU) and partner countries, in accordance with the provisions of the "Council Guidelines for Cooperation on Cyber Defense with Partners and International Organizations" (taken in August 2008) and "Framework for Cooperation on Cyber Defense between NATO and Partner countries" (taken in April 2009).

3. The present legal framework in Romania

In the light of the response to the new challenges of cyber security, Romania must fulfill the responsibilities assumed in the treaties signed with the international bodies. At the same time, this is a duty towards the safety of its own citizens in the context of the effort aimed at the development of a future Knowledge Society in Romanian.

Introduced for the first time within the national legislation, of the term "crimes perpetrated through computers" was achieved through law No. 21/1999, in order to prevent and punish money laundering (now repealed).

In 23 November 2001, in Budapest, was signed Convention on Cybercrime by the Council of Europe, which aims to prevent the acts directed against the confidentiality, integrity and availability of computer systems, networks and data, as well as the fraudulent use of such systems, networks and data. The measures proposed are designed to ensure the criminalization of such conduct and effective control of these types of crimes. At the same time, the provisions of the Convention facilitate the discovery, investigation and the prosecution of crime both nationally and internationally. The Convention was ratified by Romania by law No. 64/2004.

At the national level, the approach in the field of cyber security was materialized on May 11, 2011, through the establishment of National Response Center to Cyber Security Incidents (CERT-RO).

CERT-RO is under the coordination of the Ministry for Information Society. It is structured as a specialized entity that possesses the necessary capabilities for the prevention, identification, analysis and response to cyber incidents. In this regard, CERT-RO works with a Steering Committee made up of specialists from the Romanian Intelligence Service (SRI), the Foreign Intelligence Service (SIE), the Special Telecommunications Service (STS), Guard and Protection Service (SPP), the Ministry of National Defense (MApN), the Ministry of Internal Affairs (MAI), the National Registry Office for Classified Information (ORNISS), the National Ministry for Information Society as well as from the National Authority for

[5] „Strategy for Operating in Cyberspace”, U.S. Department of Defense, 2011.

Management and Regulation in Communications (ANCOM). CERT-RO is annually submitting an activity report to the Supreme Council of National Defense (CSAT).

Under CERT-RO was set up the Early Warning System and Real Time Information relating to cyber incidents, developed as a set of operations and technical systems with the purpose of identifying the preconditions of cyber incidents and warning in case of ontogeny.

Simultaneously with the establishment of the National Response Center to Cyber Security Incidents, the Ministry for Information Society has launched for public debate the draft entitled "Cyber Security Strategy of Romania". The document defines concepts as "cyber warfare", "cyber terrorism" and "IT criminality" and counselors for the formation of a National Cyber Security System in order to ensure the prevention, knowledge and countering an attack against the national digital space. Later, on 5 February, the CSAT has approved the Cyber Security Strategy in Romania.

Currently, the Romanian Penal Law regulates more offenses that correspond to the cybercrime domain. These are set out in Title III (*Prevention and combating cybercrime*) of Law no. 161/2003 on certain measures to ensure transparency in the exercise of public dignities, public functions and in business, the prevention and sanctioning of corruption, as well as within the Law no. 8/1996 on copyright and related rights (articles 140-143) and in Law 365/2002 on electronic commerce (articles 24-29).

Law no. 286 of 17 July 2009 concerning the Romania's New Criminal Code, which came into force with effect from February 1, 2014, makes express reference of these specific offenses in Title II - offenses against property, *Chapter IV - Fraud committed through IT&C systems and electronic payment instruments* (article 249-computer fraud; article 250 - conducting of financial transactions fraudulently and article 251-acceptance of financial transactions made fraudulently) as well as Title VII-offenses against public safety, *Chapter VI-offenses against the safety and integrity of IT systems and computer data* (article 360-illegal access to a computer system; article 361-illegal interception of computer data transmission; article 362-tampering with the integrity of the computer data; article 363-disruption of functioning information systems; article 364-unauthorized transfer of computer data and article 365-illegal operations with devices or computer software).

Instrumental in terms of preventing and countering cyber threats rests with the Romanian Intelligence Service, the national authority in the field of Cyber Intelligence. Even though the specific means and methods for neutralizing threats from cyberspace may not be disclosed, whereas the activity of intelligence is classified, preoccupations within the Service are publicly visible on the occasion of international cooperation.

In February 2011, SRI specialists attended the Cyber Cafe Conference on "Critical Infrastructure and electronic payments services"

In October 2011, the NATO headquarters in Brussels held the signing ceremony of the memorandum of understanding of security cooperation between NATO Cyber Defense Management Board and the Romanian Intelligence Service.

Conclusions

The upward trend of cyber crime and increased frequency of computer attacks requires substantial involvement of the agencies and organizations involved in the protection of national security.

This context highlights the need to consolidate a legal framework relating to cyber security, to ensure the necessary conditions for preventing and combating online attacks.

It would be a mistake to assess that the development of the Internet is causing the global escalation of computer-related crimes. However, negative developments will be cast down in the absence of a legal framework regarding cybercrime, widely accepted at international level.

BIBLIOGRAPHY:

1. Law No. 8/1996 on copyright and related rights.
2. Law No. 365/2002 on electronic commerce.
3. Law No. 161/2003 on certain measures to ensure transparency in the exercise of public dignities, public functions and in business, the prevention and sanctioning of corruption.
4. Law No. 64/2004 ratification of the Council of Europe Convention on Cybercrime;
5. Law No. 286/2009 on the new Criminal Code of Romania.
6. H.G. No. 494/2011 on the establishment of National Response Center to Cyber Security Incidents (CERT-RO).
7. HOWARD, John D., *An Analysis of Security Incidents on the Internet,* http://resources.sei.cmu.edu/asset_files/WhitePaper/1997_019_001_52455.pdf, accessed on 13 July 2014.
8. STICLARU, Marius, „Securitatea cibernetică – prioritate a sectorului de intelligence în lumea globalizată*",* în *Revista Intelligence,* nr. 20, Sept-Oct. 2011.
9. The European Commission, *„Towards a general policy on the fight against cyber crime"*, COM(2007), 267.
10. „Strategy for Operating in Cyberspace", U.S. Department of Defense, 2011.
11. DOBRINOIU, M., *Infracţiuni în domeniul informatic*, Editura C. H. Beck, Bucuresti, 2006.
12. SINROD, E.J.; REILLY, W.P., „*Cyber-Crimes - "Computerul şi tehnologia înaltă*", Santa Clara, Law Journal, 2008.
13. *Cisco 2013 Annual Security Report,* accessed on 4 July 2014 at http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_ 2014.pdf..
14. http://www.b1.ro/stiri/high-tech/bitdefender-avertizeaza-cu-privire-la-un-atac-cibernetic-care-indeamna-la-atacarea-site-urilor-guvernamentale-din-occident-care-au-impus-sanc-iuni-rusiei-90526.html, accessed on 7 September 2014.
15. www. agerpres.ro din 13 ianuarie 2013, accessed on 10 August 2014.
16. www. agerpres.ro din 16 ianuarie 2013 accessed on 10 August 2014.
17. www.sri.ro din 10.08.2014, accessed on 18 August 2014.
18. www.sri.ro din 11.08.2014, accessed on 18 August 2014.

CYBER THREATS TO NATIONAL CRITICAL INFRASTRUCTURES

Silvia-Alexandra MATACHE ZAHARIA
PhD candidate, National Security and Information, "Carol I" National Defence University, Bucharest, Romania.
E-mail address: silvialex.zaharia@yahoo.com

Abstract: *The information age has generated substantial shifts in the way economic, social and military actions are conducted by international actors. Easy access to information and communication technologies represents one of the basic features of contemporary society, and the development level of IT&C equally affects government institutions, the business sector and the everyday life of individuals. Critical infrastructures are also affected by this phenomenon of increased informatization as they comprise, for their larger part, computers or other information-based components. From this point of view, the protection of critical infrastructures against cyber threats represents a sine qua non requirement for ensuring national security, with major implications on the social and economic development. The present paper wishes to outline the main cyber threats with which national critical infrastructure networks and systems are confronted. Furthermore, the paper intents to present the main regulations of the National Strategy for Cyber Security and to analyze the way in which they can be applied to the area of national critical infrastructure protection.*

Keywords: *critical infrastructures, cyber security, protection, cyber threats.*

Introduction

The last thirty years or so have been characterized by the rapid development of all sorts of information and communication technologies, which transformed the fabric of social and economic interactions all over the world. The world's increasing dependence on computers changed social paradigms, philosophies, economies, defence, and ultimately everyday life to such an extent that nowadays, it is practically impossible to ensure the normal functioning of society without IT&C, or even to imagine that such a thing would still be possible. The paradox of this situation is that, the more a society depends on computers and on IT&C technology, the more developed and at the same time vulnerable it is.

This increased informatization of all layers of social, economic, cultural and military interactions has created a new phenomenon called virtual reality or cyberspace. Some of the main characteristics of the cyberspace are its dynamic evolution, the anonymity of users, the lack of physical frontiers as well as the relative absence of rules and regulations. These traits contributed to the development of IT&C, but also can constitute risk factors to the normal functioning of individuals, states or even of cross border organizations. The benefits of a computerized society are thus countered by increasing systemic vulnerabilities and internal threats (cyber threats).

In this context, ensuring the security of the cyberspace as a whole as well as one's security while acting within the „boundaries" of virtual reality has become a major preoccupation of individuals, states and international actors. The issue of cyber security has increasingly demanded institutional responsibility, as governments took the course of elaborating and implementing coherent policies in the field.

Critical infrastructures are also an essential part of a well-functioning, developed society. As they also developed and improved in later years, they have come to depend on

IT&C as much as other sectors of the economy and to accommodate computers, network systems and other IT components. These vital infrastructures need special protection measures in order to ensure their proper functioning and to fulfil their role as vital components that fuel the well-being of society. Implicitly, these security measures include actions that prevent and/or counter cyber threats.

The present paper wishes to bring into the limelight some of the most frequent cyber threats to national critical infrastructures, and to discuss how actions and plans aimed to prevent them fit in the wider framework of the European and national strategy for cyber security.

1. Strategic Perspectives on Cyber Security

Governments all over the world attempt to tackle the issue of cyber security, as new cyber threats and vulnerabilities of IT&C emerge almost daily. The coordination of government action with private sector initiatives is crucial for ensuring an effective framework for a strategic approach to cyber security, generally accepted as being the "state of normalcy resulted after implementing an ensemble of proactive and reactive measures"[1] meant to ensure the confidentiality, integrity, availability and authenticity of cyber information, resources and services.

Recent cyber-attacks on European critical infrastructures have proved to be extremely costly, both for governmental institutions and for the business environment. A perfect example is the series of cyber-attacks on Estonia that took place in 2007. The attacks paralyzed the country's communication systems, Internet sites, the banking system and the integrity of civil and private information systems of Estonian citizens, causing financial damages estimated at more than 10 million Euros[2]. A closer look on these attacks reveals that they were launched on the 27th of April, at the same time when street protests by Russian ethnics against the government's decision to move a WWII statue representing a Russian soldier began. The websites of governmental institutions and public services (including the websites of the Presidency, the Government, the Prime Minister, all Ministries except the webpage of the Ministry of Culture, the Parliament, the Police, Mayor offices all over the country and other local services), the banking sector and news portals were assaulted and, ultimately, blocked by predominantly denial-of-service (DoS and DDoS) attacks. Practically, the websites were "bombarded by mass requests for information - overwhelming their computer servers"[3]. Moreover, mail servers of the chosen targets were „flooded" with spam e-mail.

The following days the cyber-attacks intensified and diversified, including a wide array of targets and using various techniques such as Internet propaganda, malicious blog comments and website deterioration. For a brief while, even the country's main emergency number was out of order. As a result of the attacks, "in some cases, officials have simply blocked access to the servers from outside Estonia, to prevent them from being attacked"[4]. The only data traceable about the series of attacks revealed that they originated from 178 states, most of them coming from the territory of the Russian Federation.

---

[1] Che-Wooi TEN, Govindarasu MANIMARAN, Chen-Ching LIU, „Cybersecurity for Critical Infrastructures: Attack and Defense Modeling" in *IEEE Transactions on Systems, Man and Cybernetics – Part A: Systems and Humans,* vol. 40, No.4, July 2010, p. 853.

[2] Sebastian CIOCAN, "Atacurile cibernetice din Estonia (2007)"(*Cyber Attacks on Estonia(2007)*), available at http://www.cssp.ro/analize/2012/10/01/atacurile-cibernetice-din-estonia-2007/ , accessed on the 27th of August 2014.

[3] "Estonia hit by 'Moscow cyber war'", available at http://news.bbc.co.uk/2/hi/europe/6665145.stm, accessed on the 27th of August 2014.

[4] *Ibidem.*

The cyber- attacks on Estonia have shown, at a European level, the destructive, long-term effects a lack of an efficient strategy for cyber security might have on the functioning of critical infrastructures, and implicitly on the economy and the state apparatus.

1.1. The European Strategy for Cyber Security

At the level of the European Union, the success of ensuring a certain degree of resilience for an effective cyber security strategy largely depends on the way in which Member States are able to coordinate their efforts for protecting vital infrastructures against cyber threats. Moreover, the necessity of adopting a European policy concerning the fight against cybercrime became stringent, as national and EU economies were more and more affected by this phenomenon.

In 2013, actions were taken to elaborate a strategic approach to cyber security and to harmonize Member States' policies dealing with cyber threats and IT&C critical infrastructure protection. These actions resulted in The Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace. The initiative was a joint effort of the European Commission and of the EU High Representative for Foreign Affairs and Security Policy, and represents the first ample document of the European Union concerning cyber security. The Strategy was accompanied by other technical and legislative proposals that were meant to consolidate the security of European critical IT&C infrastructures. The document offered a set of priorities for EU policies concerning cyberspace, which include the following[5]: freedom and openness, readiness to represent the vision and the principles of the EU in the virtual space as well as in the material world; establishing a coherent international EU policy concerning cyber space; applicability of EU laws, norms and fundamental values in cyber space and shared responsibility al all participants to the global information society for ensuring cyber security; reducing cybercrime; developing and consolidating European cyber security capabilities, collaborating with international organizations, private sector and civil society representatives in order to secure the IT&C critical infrastructures in non-EU countries; developing industrial and technological cyber security resources, promoting a single market for cyber security products and fostering innovation and research investments; improving and easing access to information and data while, at the same time, preventing cyber threats; obtaining a resilient critical cyber infrastructure; establishing a defence policy against cyber-attacks, within the wider framework offered by the Common Security and Defence Policy; last but not least, encouraging international cooperation in the field of cyber security, since preserving an open, free, yet secure cyber space represents a global challenge.

The Strategy was accompanied by other legislative proposals concerning attacks against IT&C systems (such as the proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union), by launching, in January 2013, a European Cybercrime Centre, and by forming a global alliance against sexual abuses of children committed via the Internet. Last but not least, the Strategy seeks to develop and finance a network of national excellence centers against cybercrime.

The above-mentioned Directive represents a key-component of the global strategy and would impose on all Member States, major Internet services operators and critical infrastructures operators, the obligation to assure a secure and resilient digital environment

[5] "The Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", p. 4-16, available at http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf , accessed on the 29th of August 2014.

throughout the European Union common space. Some of the proposed measures[6] of the Directive include: the obligation of all Member States to elaborate and implement a security strategy for IT&C networks and to designate a competent national authority that would have the human and financial resources for preventing, managing and resolving security incidents; the creation of a cooperation mechanism between Member States and the Commission for issuing early warnings via a secured infrastructure and to organize periodic inter pares evaluations; and last, but not least, the obligation of critical infrastructure operators from the finance, transports, energy and health sectors, service operators from the IT&C industry (app stores, e-commerce platforms, Internet payments, cloud computing, search engines and social networks) and public administrations to adopt risk management practices and to report major security incidents.

It can be stated that the EU Cyber Security Strategy and the Directive proposal represent attempts of promoting a unitary, coherent approach on the best ways to prevent cyber threats and to manage disturbances caused by cyber-attacks. Their aim is to promote European values, such as freedom and democracy, and to ensure a safer development of a profitable cyber economy. The international policy of the EU concerning cyber space wishes to enforce a responsible behavior for all users, supporting the enforcement of international legislation concerning cybercrime and assisting non-EU states in consolidating their cyber security capacities.

As a member of the European Union, Romania supports an integrated, common approach to cyber security. Our country aims to develop a dynamic IT&C sector and to create an adequate legal framework for it, one that would be based on the interoperability of core services, respect for the fundamental rights and freedoms of citizens and the preservation of national security interests.

1.2. Romania's National Cyber Security Strategy

Taking into consideration the multitude of risks and threats to cyber security and the dynamic evolution of the IT&C sector has prompted Romanian authorities to take certain steps for developing a cyber-security culture for private and state users, and for implementing measures to counter potential threats. The Romanian government assumed a coordinating role for national activities and initiatives concerning cyber security, in accordance with the measures taken by NATO and the EU. As a result of this decision, in 2013, the government approved, not without some criticisms from NGOs and some representatives of civil society, the National Strategy for Cyber Security and an Action Plan concerning the implementation of a National Cyber Security System.

The National Cyber Security Strategy respects the guidelines of the EU and NATO strategic perspectives on cyber security. Its purpose is to define and maintain a safe virtual environment, with a high degree of resilience. The protection of national critical infrastructures that use IT&C technologies and services is crucial for national security and good governance, as well as for the business environment and for social welfare.

In order to assure a coherent and efficient security framework, the strategy adheres to the principles and objectives of the National Defence Strategy and of the National Strategy for the Protection of Critical Infrastructures. It envisions several steps[7] that must be taken for

[6] " Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network an information security across the Union", p. 19 – 25 available at http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_en.pdf, accessed on the 27th of August 2014.

[7]"HGR nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică", published in *Monitorul Oficial,* Part I, no.296/23.05.2013, p.6, available at http://www.cert-ro.eu/files/doc/Strategia DeSecuritateCiberneticaARomaniei.pdf , accessed on the 29th of August 2014.

ensuring cyber security, such as: adapting the legislative and institutional framework of the country to the dynamics of existing and emerging cyber threats; establishing and implementing a set of minimal security requirements for national critical infrastructures, that are both efficient at countering potential cyber threats and relevant for the proper functioning of the vital infrastructure components; ensuring the resilience and development of cyber infrastructures; taking advantage of the opportunities offered by the cyberspace to promote national interests and objectives; maintaining a state of security by understanding, preventing and countering vulnerabilities, risks and threats to Romania's cyber security; promoting and developing international cooperation, as well as the collaboration between the public and private sectors at a national level for researching and improving the means of maintaining cyber security; developing a security culture amongst the population by revealing the vulnerabilities of the IT&C sector, the risks and threats emerging from cyber space, and the necessity to protect their own computer systems; actively participating in the initiatives of the international organizations that Romania is part of in order to define cyber security and to set up a guideline for instituting efficient protection measures.

According to the Strategy, the general cooperation framework for cyber security, comprising public institutions and authorities with responsibilities in this area, is called the National Cyber Security System, and it acts on several levels: identification, prevention, cooperation and coordination, and countering[8]. At a strategic level, the System's activity is coordinated by the Supreme Council for National Defence, which approved the organization and functioning of an Operative Council for Cyber Security, formed by representatives from the Ministry of National Defence, the Ministry of Internal Affairs, the Ministry of Foreign Affairs, the Ministry for Information Society, The Romanian Intelligence Service, the Special Telecommunications Service, the External Intelligence Service and other organisms with similar responsibilities. Furthermore, the National Response Centre for Cyber Security Incidents, which was established in 2011, elaborates and disseminates public policies to prevent and counter cyber threats to national infrastructures.

As it can be observed, in the past few years, despite internal criticisms and popular scepticism, Romania took major steps concerning cyber security. Our country seems eager to cooperate with other regional or international organisms, in order to improve the safety level of cyber critical infrastructures. According to some authors, one of the most important lessons that Romania can and must learn from wider cooperation formats concerning cyber security is to "adapt and permanently upgrade its capabilities, in order to be able to face the technological advances made by potential adversaries and to counter new cyber-attack methods"[9]. The simplest way to achieve this desiderate in a cost efficient manner is to adopt widely accepted standards for data security, risk assessment, and designing security management systems.

Furthermore, our country seems eager to assume a regional role in ensuring cyber security, despite the novelty of its own strategic approach on the issue. Even though our country's cyber security strategy is barely a year old, Romania recently expressed, during the NATO Summit in Wales, its willingness to be „leading nation"[10] for a Trust Fund meant to aid the development of Ukraine's cyber defence capabilities. Our country's readiness to raise funds and promote cyber security projects shows confidence in Romania's capabilities for

[8] *Ibidem,* p. 12-13.

[9] Gabriel TRIȚESCU, "Capabilități cibernetice ale NATO şi ale României – trecut, prezent şi viitor" in *Revista comunicațiilor şi informaticii*, no.2/2013, edited by the „Decebal" Training Center for Communications and Informatics, Sibiu, 2013, p.50.

[10] "Obiectivele României la Summitul NATO", available at http://www.digi24.ro/Stiri/Digi24/Special/NATO +-+SUMMITUL+SECURITATII+MONDIALE/Obiectivele+Romaniei+la+Summitul+NATO , accessed on the 4th of September 2014.

cyber defence. Perhaps the experience in promoting a national strategy on the issue and the investments in IT&C security technologies would prove a sufficient guarantee for becoming a regional leader in promoting cyber security.

2. Cyber Threats to National Critical Infrastructures

A quick overview on cyber security reveals that there are more than 150 000 computer viruses that "roam" the web and approximately 148 000 computers that are compromised daily, with a high probability that critical infrastructures would be affected, which could cause serious financial damages. A great deal of cyber security incidents are caused by cybercrime.

As it was stated earlier, most critical infrastructures have at least some computerized components that are connected to other computer networks or even to the Internet. The interconnectivity of these computer systems makes them vulnerable to a whole array of cyber threats, coming from various sources. These cyber threats can affect both hardware and software components of a computer system.

The vulnerabilities created by the interconnectivity of critical infrastructures allow potential cyber attackers to act from a distance to destabilize the system. And since, with the advent of the Internet, a great deal of information in available to the wider public, these vulnerabilities can easily be identified by almost anyone with the aid of exploit tools and can be used to facilitate the hacking of the targeted computer system of any given critical infrastructure.

2.1. Potential Sources of Cyber Threats

Cyber threats and cyber-attacks are almost a permanent feature of the virtual world. The cyber confrontation or cyber war is a subversive method used by both state and non-state actors to undermine the resilience of potential adversaries by paralyzing their computer – based critical infrastructure. Cyber confrontations are especially complex, which makes them hard to define and recognize. However, there are some characteristics of cyber wars[11] that can be identified: the difficulty in identifying one's adversaries; the continuity of the threats; the absence of physical, geographical and temporal frontiers; the multitude of possible targets; the lack of a clear set of warning indicators; the absence of rapid remedies for the consequences caused by a cyber-attack; the use of a relatively accessible technology; the difficulty in establishing clear and precise responsibilities for cyber security management; the relatively low costs of cyber operations (cyber ops); increased manipulation possibilities.

A primary classification of cyber threats reveals that they can be unintentional or intentional. Unintentional threats can emerge from software upgrades or maintenance procedures that are done in a careless manner and can affect the system. Intentional cyber threats can be directed or non-directed, and can originate from some of the following sources[12]:

a) *Bot-net operators*, who use remotely controlled networks of compromised systems in order to coordinate attacks;

---

[11] Dan ŢIBULIAC, Gelu-Cătălin POPA, „Războiul cibernetic şi securitatea informatică" in *Revista comunicaţiilor şi informaticii*, no.2/2013, edited by the „Decebal" Training Center for Communications and Informatics, Sibiu, 2013, p.47.

[12] Constantin MINCU, Gruia TIMOFTE, „Riscuri şi ameninţări din spaţiul cibernetic din spaţiul cibernetic la adresa infrastructurii informaţionale critice" in *Lucrările conferinţelor,* vol.4, 2011, no. 2, The Scientific Fall Session of the „Universe of Science" Center, Mioveni, Argeş County, 8-10 September 2011, The Protection of Critical Infrastructures Section, The Romanian Scientists' Academy Publishing House, Bucharest, 2012, p.65-66

b) Organized criminal groups, that attack computer systems to obtain financial gains;

c) Hackers, who attack computer systems from the outside and can compromise vital cyber infrastructures for "fun" or to prove themselves in front of hacker communities;

d) Insiders, that have an in-depth knowledge of the targeted system, can override safety measures and have unrestricted access to essential data. In this category, one can include employees, system operators or private contractors that ensure the maintenance of the system;

e) Phishers, or data collectors, who try to steal identities or private information for financial gains;

f) Spammers, who send unsolicited e-mails with hidden or false information in order to sell products, conduct phishing schemes, or distribute spyware or malware meant to facilitate the attack on the system;

g) Cyber terrorists who, by using cyber-attacks such as phishing schemes or spyware/malware, collect confidential data that can be used to damage or destroy critical infrastructures in order to threaten national security.

To the above mentioned categories, one might add *states* as a potential source of cyber threats. States have the capability of using cyber-attacks for espionage and collecting confidential data or can develop cyber war capacities in order to destroy the critical infrastructures of other rival states.

The diversity of sources can generate a vast typology of cyber threats and cyber-attacks to critical infrastructures. The dynamics of the cyber space, which evolves and changes at a very rapid pace, can sometimes make it difficult to assess all potential threats to a vital infrastructure and/or to have a complete, exhaustive classification of cyber – attacks. Theoretic attempts to categorize them are doomed to portray only a small part of the greater picture. However, a theoretic approach on defining and classifying cyber threats is necessary in order to develop a coherent strategy to counter them.

2.2. A Typology of the Most Common Cyber Threats to Critical Infrastructures

Cyber threats can generally affect computer networks, servers, network connections, service providers, individual computers as well as other physical infrastructures such as buildings, energy networks, cables and other computer components, as well as software, data basis and other computer programs. A basic classification of risks and threats to national critical infrastructures that emerge from the cyber space can include[13]: risks and threats derived from economic competition between companies for resources and market share in the IT&C industry; asymmetric threats, such as cyber terrorism; the development of unconventional and subversive IT&C networks, such as TOR; hacking.

A more detailed classification of cyber threats comprises the following types of harmful activities:

a) *Denial-of-service*(DoS) attacks can stop a system to execute the data exchange, thus disturbing the activity of the infrastructure served by the targeted computer network. This type of attack regularly comes from a single source and prevents the legitimate users from accessing the system by blocking data traffic and jamming the targeted computer with messages. A variation of this type of cyber threat is the *distributed denial-of-service* (DDoS), in which the aggression is coordinated by a distributed computer system;

b) *Logic Bombs,* consist of specific codes that are inserted by the system's programmer and that can become destructive if certain logical conditions are fulfilled;

c) *Phishing* is represented by the creation and use of e-mails and websites – designed in such a manner as to look extremely similar to the sites of legitimate businesses, financial

[13]Grigore ALEXANDRESCU, Gheorghe VĂDUVA, *Infrastructuri critice. Pericole, ameninţări la adresa acestora. Sisteme de protecţie,* „Carol I" National Defence University Publishing, Bucharest, 2006, p.36.

institutions or well-known government institutions – to mislead users and determine them to reveal personal data such as passwords or banking accounts numbers. The information thus obtained is usually used for identity thefts and financial frauds;

d) *Sniffer*, is a software that intercepts exchanged data and examines each data package searching for specific information;

e) *A Trojan,* is a software that hides malicious code, or malware. Usually, a Trojan is disguised in a useful software, one that a user is willing to install and execute;

f) *A Virus,* is a software that infects computer files, most commonly those with the extension .exe (executable files) by inserting a copy of itself within the file. The copy is then executed when the infected file is loaded, thus allowing the virus to infect other files.

g) *Vishing,* is a phishing scheme used on Voice-over-Internet Protocol(VoIP) technology and on the software of open-source call centers that allows cyber criminals to create false call centers that can send e-mails and text messages to users requesting them personal data such as banking or financial accounts;

h) *War driving* is a method to obtain unauthorized access to wireless networks by using a laptop, antennas and a wireless network adaptor;

i) *A worm* is an independent computer program that reproduces itself by self-copy from a computer to another, given the targeted computers are connected to each other via a network. Unlike viruses, worms do not need human intervention in order to multiply and spread;

j) *Zero- day exploit* is a cyber-threat that takes advantage of a system's vulnerability in the same day that the vulnerability is revealed to the general public and that, until now, cannot be prevented.

Apart from the threats mentioned above, there are other common cyber threats such as: inadequate system monitoring, inefficient protection measures, unexpected expansions or interconnections of a given computer system or operating errors made by human users. They usually incite less attention but, nonetheless, can prove equally harmful to the security of national critical infrastructures.

Conclusion

The multitude of possible cyber threats to critical infrastructures reveals the challenging nature of ensuring the protection and security of these vital components. As it can be observed, a strategic approach to cyber security is necessary, and it is our belief that an efficient strategy in this domain requires an intensive collaboration between private and public sectors. Since the threats to cyber infrastructure can emerge from a variety of sources, the proficient management of risk assessment and prevention can only be done jointly, by exchanging information, conducting security exercises and crisis simulations, and sharing resources.

First of all, the exchange of information allows private and governmental partners to correctly evaluate events, analyze risks and determine appropriate courses of action. Secondly, simulations and exercises contribute to the maintenance of organizational expertise and can prove to be a decisive test for determining the quality of institutional interactions in the event of a serious cyber-attack. Last, but not least, sharing the resources contributes to the maximization of profit and optimization of their use, representing a key element for the protection of national critical infrastructures against cyber threats.

Acknowledgement:

This work was possible with the financial support of the Sectoral Operational Programme for Human Resources Development 2007-2013, co-financed by the European

Social Fund, under the project number POSDRU/159/1.5/S/138822 with the title ***"Transnational network of integrated management of intelligent doctoral and postdoctoral research in the fields of Military Science, Security and Intelligence, Public order and National Security – Continuous formation programme for elite researchers - "SmartSPODAS"."***

BIBLIOGRAPHY:

1. "Obiectivele României la Summitul NATO", available at http://www.digi24.ro /Stiri/Digi24/Special/NATO++SUMMITUL+SECURITATII+MONDIALE/Obiectivele+Romaniei+la+Summitul+NATO.
2. "Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network an information security across the Union", available at http://eeas.europa.eu/policies/eu-cyber-security/cybsec_ directive en.pdf.
3. "Estonia hit by 'Moscow cyber war'", available at http://news.bbc.co.uk/2/ hi/europe/6665145.stm.
4. "The Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", available at http://eeas.europa.eu/policies/eu-cyber-security/cybsec_ comm_en.pdf .
5. "HGR nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică", published in *Monitorul Oficial ,* Part I, no.296/23.05.2013, available at http://www.cert-ro.eu/files/doc/StrategiaDeSecuritate Ciberne ticaARomaniei.pdf.
6. ALEXANDRESCU, Grigore, VĂDUVA, Gheorghe, *Infrastructuri critice. Pericole, ameninţări la adresa acestora. Sisteme de protecţie,* „Carol I" National Defence University Publishing, Bucharest, 2006.
7. CIOCAN, Sebastian, „Atacurile cibernetice din Estonia (2007)"(*Cyber Attacks on Estonia(2007)*), available at http://www.cssp.ro/analize/2012/10/01/atacurile-cibernetice-din-estonia-2007/ .
8. MINCU, Constantin, TIMOFTE, Gruia, „Riscuri şi ameninţări din spaţiul cibernetic din spaţiul cibernetic la adresa infrastructurii informaţionale critice" in *Lucrările conferinţelor,* vol.4, 2011, no. 2, The Scientific Fall Session of the „Universe of Science" Center, Mioveni, Argeş County, 8-10 September 2011, The Protection of Critical Infrastructures Section, The Romanian Scientists' Academy Publishing House, Bucharest, 2012.
9. TEN, Che-Wooi, MANIMARAN, Govindarasu, LIU, Chen-Ching, „Cybersecurity for Critical Infrastructures: Attack and Defense Modeling" in *IEEE Transactions on Systems, Man and Cybernetics – Part A: Systems and Humans,* vol. 40, No.4, July 2010.
10. TRIŢESCU, Gabriel, "Capabilităţi cibernetice ale NATO şi ale României – trecut, prezent şi viitor" in *Revista comunicaţiilor şi informaticii*, no.2/2013, edited by the „Decebal" Training Center for Communications and Informatics, Sibiu, 2013.
11. ŢIBULIAC, Dan, POPA, Gelu-Cătălin, „Războiul cibernetic şi securitatea informatică" in *Revista comunicaţiilor şi informaticii*, no.2/2013, edited by the „Decebal" Training Center for Communications and Informatics, Sibiu, 2013.

SECURING CRITICAL INFRASTRUCTURES – PRIORITY OF THE ROMANIAN STATE IN THE CONTEXT OF NEW CYBERNETIC THREATS

Olguţa DOGARU
Chief commisioner, specialist officer, PhD, "Alexandru Ioan Cuza" Police Academy, Bucharest, Romania.
E-mail address: olgutadogaru@yahoo.com

Abstract: *Securing critical infrastructures entails a long-term and coherent partnership among critical infrastructure owners, the personnel in charge of managing and monitoring them, public and private authorities as well as European Union member states with a view to creating and enforcing a consistent legal framework.*

Keywords: *cyber threats, cyber shield, critical national infrastructures, strategic war, computer espionage.*

Introduction

While compiling statistic of operations during the last years, characterized by an increase and a diversity of the fields where cyber threats have posed risks to, cyber security specialists outlined their asymmetry as a main feature. To put it differently, they are *non-conventional, dynamic*, sometimes *random* and *non-linear*, *difficult to quantify and forecast* while the perpetrators of them are specialized in accordance with the purpose of their operations. They can range from simple natural persons engrossed in computing and willing to show off their abilities to traffickers, terrorists, spies, extremists and religious fanatics and even corrupt employees of financial institutions.

Unlike classical threats that the specialists are trained to deal with, cyber threats differentiate themselves by: "deep uncertainty as regards their opponents' objects, speed and the level of spreading of the operation."[1].

The incapacity to assess the damages caused by the spread of information via communication systems to the systems of all parties that are connected thereto makes the actual losses extremely difficult to ascertain.

The Director of the National Security Agency of the USA, James Clapper, stated before the American Senate upon the submission of the annual Report on the dangers the country is exposed to: "in certain cases, people apply digital technologies at a speed which is higher than our capacity to understand the implications of it for our national security or to try to mitigate its risks."[2] Thus, he admitted that the speed at which information technology evolves tends to pose difficulties to security experts.

When we approach the issues of cyber threats to critical infrastructures by having in view both the current reality and the perspective of a future that does not give us the time to postpone the elaboration of coherent strategies to face such threats, the challenge that was

[1] George Maior and collaborators, *Un război al minţii - Intelligence, servicii de informaţii şi cunoaştere strategică în secolul XXI* (A mind war - Intelligence, intelligence services and strategic knowledge in the XXIst century), RAO Publishing House, Bucharest, 2010, p. 237.

[2] Ioan Hurdubaie, *Atacurile cibernetice înlocuiesc terorismul ca primă ameninţare pentru Statele Unite ale Americii*, in „Ultima oră" newspaper, 25 March 2013, http://www.optimalmedia.ro/poveste/atacurile-cibernetice-înlocuiesc-terorismul-ca-prima-ameninţare-pentru-statele-unite-ale-americii/7013.

launched before all the states of the world is perfectly justified if we take into account that: "The security for the future shall not be gained only by using weapons but by gaining complete settlement among all the countries. The 9/11 events increased our progress towards ensuring a safer future. From this moment on, we must acknowledge that security has become a worthy asset that must be well nurtured, protected and administered if we want to survive. We will be compelled to change, to exit denial, to work together and unite our efforts. We must be prepared to face the future with all its challenges."[3].

As far as national security policies are concerned, globalization compels the states to integrate their security policies. As member of N.A.T.O and UE, Romanian security has become N.A.T.O's and UE's security. The obligations it undertook as a member state trigger the harmonization of the Romanian national security strategy with the objectives set out by NATO's strategic Concept and UE's Security Strategy"[4].

Pursuant to the European Security Strategy, the security of a nation is defined by the following five dimensions: political, military, economic, diplomatic and environment protection. To this respect, the cyber security of infrastructures represents a challenge to all the above mentioned five dimensions which imposes a global approach through both a national cooperation among public, private institutions and NGOs and an international cooperation among organizations, regional and global institutions.

The spread of cyber threats has alarmed decision-makers all across the globe having significant implication not only from the point of view of financial losses but also due to the fact that they endanger national security.

Following the heavy cyber-attacks our country has been subject to for the past year, the Romanian authorities realized they should not neglect their implications that highly jeopardize the national security.

Hence, presidential counselor on security, Iulian Fota, stated at an event on cyber security: "having in view the statistics for the past year, it is possible that cyber security should become our second major concern after terrorism" and that "it has become very clear that at this point security has gain another meaning. We will not address the issue of security only from a military or intelligence perspective and we have to add a new dimension: cyber security"[5]. In consequence, at this moment, besides its old dimensions, national security commences to comprise cyber security.

1. Critical infrastructure – the vital structure of society

According to the National Strategy of Romanian Defense (SNAp), infrastructure is defined as: "the system of *material elements* (constructions, equipment, installation, transportation means, material benchmarks valued symbolically), *organizational elements* (transportation and communication networks, energy systems, supply systems, education and health systems) and *informational elements* (data, intelligence, fluxes, circuits techniques and procedures) that form a social macro-system ensuring its operation and viability in the general context of social development"[6].

If such infrastructure is inefficiently protected and managed, this may lead to critical situations that may hamper its operation and have severe consequences upon national security.

---

[3] James Canton, *Provocările viitorului* (Future Challenges), Polirom Publishing House, Bucharest, 2010, p. 245.
[4] Cristian Troncotă and collaborators, *Neliniştile insecurităţii* (Insecurity Anxieties), Tritonic Publishing House, Bucharest, 2005, p. 19.
[5] National Forum on Security, 2nd Edition, *Cyber Security*, organised by „Carol I" National Defence University, Bucharest, 21-22 October 2013.
[6] *National Defence Strategy*, 2010, p. 26.

In the same document, critical infrastructure is also defined as: "any operational economic entity that offers products/ goods and public utility services which are vital to the entire society, whose destruction, degradation or non-operation shall produce a major impact upon both population and economy at a national or regional scale."

The development and the proper operation of a state depend on the security of its infrastructures because, in general, infrastructures and, in particular, critical infrastructures represent the core of modern and developed societies. Therefore, they have always been the most sensitive and vulnerable structure in any society.

If we generalize the term "infrastructure" we tend to refer to all component structures of a state starting with its inhabitants; such structures takes either separately or as a whole enable the performance of the economy and of the society.

Therefore, all vital structures are included in the category of critical infrastructures: *electrical systems, nuclear objectives and installations, information technology and communication systems, extraction systems, processing systems, storing and transportation of primary energy sources, water supply systems, infrastructure and communication means, banking, financial and insurance systems, health services, intervention in critical situations, public values and utilities and public authorities.*

The global spread of information technology systems and of further means of communication within critical infrastructures, the speedy access and the possibility of interconnection of different databases resulted in the fact that strategic structures depend on all the above enumerated causing easily exploitable vulnerabilities.

Cyber-attacks against critical infrastructures may cause disasters if we take into consideration the fact that these are controlled and operate on the basis of information technology components and any interference is likely to hinder the operation of the infrastructure system.

Used for attacks against critical infrastructure objectives such as nuclear stations, financial institutions and transportation system, the prominence of cyber-attacks outline how important it is to improve the response of the responsible authorities.

Professor Scott Kemp from the Department of Engineering and Nuclear Science of the famous Massachusetts Institute of Technology (M.I.T.), states: "Cyberweapons do not appear to be capable of mass destruction in the way nuclear weapons clearly are, but they hold at risk some of the most precious assets of our time: the information storage and control mechanisms on which modern society has been built"[7].

To this respect, it should not be difficult to envisage the huge damage caused by an error code in the banking, energy, nuclear or health system.

The growth in increasingly sophisticated cyber attacks has come to constitute a real threat to economic institutions, economy and national security.

In this regard, measures are required to assess the entirety of potential risks and strategy development to include counteraction and damage mitigation.

To meet such goals, activities carried out by every facility and component system ensuring critical, national-stake infrastructure protection, need to undergo monitoring.

At the same time, training of cyber safety experts, massive investments in equipment and security technology, doubled by joint efforts of public, private environments and civil society representatives become prerequisites in creating a functional "trinity" capital to the existence and development of a nation-wide strategic cyber infrastructure.

Thus, critical infrastructure represents a national security asset on whose smooth operation and viability depends the sheer existence of our society which is why the *basic*

[7] R. Scott Kemp, *Cyberweapons: Bold steps in a digital darkness?*, in "The Bulletin of the Atomic Scientists", June 7, 2012.

principle of the protection concept of critical infrastructures is *cooperation* at all levels between the responsible public authorities and private partners in order to attain stability and national security.

By applying this principle at a global level, we can conclude that in order to protect themselves against such threats, the states need to share information in the field of cyber security and the legislation should be enforced with a view to combating cross-border criminality.

It is a foregone conclusion on which PhD Joss Wright from Oxford Internet Institute, cited by BBC News Agency, comments: "The recommendations have been endlessly repeated by certain people for the past 1o years. I would like to see that sharing information will take off but when it comes to national security there is a culture that prevents us from sharing. No one can change all of a sudden 70 – 100 – 1000 years of military thinking".[8]

Nevertheless, as Romanian Intelligence Agency Director, George C. Maior outlined: "replacing the classical premises of *need to know* by *need to share* is, still, for many countries hard to pass through from the everyday reality in which different organizations maintain their own knowledge as an exclusive and autarchic privilege meant to consolidate their own prestige and interests for public administration"[9].

By adapting old intelligence principles characteristic to field operations to the reality of our times, we will soon realize that in order to fight against virtual threats the states will have to reunite their efforts and increase research and development to prevent and combat cyber-attacks although such actions may also entail precautions and doubts.

The risks and the threats that the states will have to deal with, will be more and more interdependent, transnational and complex by their very nature which will trigger tighter international, bilateral, multilateral, regional and global cooperation.

The greatest challenge faced by international authorities when combating such phenomenon remains its complexity. It is very difficult to identify the culprit, such crimes are hard to monitor due to the superior equipment the perpetrators possess and sometimes it is even more strenuous due to security issues that very from one state to another – when the perpetrator is located in another state; this is why the fight against criminality has global perspectives which impose aligning legislative provisions and updating cyber security strategies.

For the time being, most of cyber threats affect companies and governmental organizations that are involved in producing weapons, or in financial operations or legal research activities in fields such as hi-tech, health and technology.

According to the latest Report of Kaspersky Lab, the software company that produces security programs, the prospects are not too encouraging. The specialists draw our attention to the fact that: "companies operating in fields such as: extraction of natural resources, energy, transportation, food industry, pharmaceuticals will be affected and so will be those dealing with securing information"[10].

It is not excluded for the next cyber threat to be a combination between cyber-attacks and physical attacks taking into consideration the fact that compromising a critical infrastructure would enable the launch of a traditional attack.

---

[8] Dave Lee, *Israel tops cyber-readiness poll but China lags behind*, in BBC News Technology, 30 January 2010, http://www.bbc.com/news/technology-16787509.

[9] George Maior and collaborators, *op. cit.*, 2010, p. 28.

[10] Alexander Gostev, *Cyberthreat Forecast for 2012*, 22 December 2011, http://laptopnews.ro/atacuri-cu-tinte-stabilite-razboi-cibernetic-amenintari-mobile-predictie-pentru-2012.html.

2. Ways in which cyber-attacks may harm critical infrastructures

Cyber threats represent a real threat and manifest through cyber-attacks against the vital infrastructure of a country. The competent institutions that handle the protection of such infrastructures are the country's security structures and data protection (public and private institutions). Nonetheless, the examination of the source of the attack, of the perpetrators' motivation and of the consequences is performed by intelligence services.

2.1. Cyber-terrorism

While *classic terrorism*, as it was defined by J. Canton is: „a non-conventional war fought in the war of innocent civilians who will be used to exert pressure on those who have the power so that they would satisfy the demands of the terrorists"[11], *cyber-terrorism* refers to illegal attacks against networks and stored information systems with a view to intimidating and exercising pressure on a government to take certain political and social measures. Depending on the created impact, *attacks against critical infrastructures may be considered attacks that are specific to cyber-terrorism***.**

A cyber-terrorist attack aims at penetrating technological resources with a view to taking control or affecting the critical elements of the national infrastructure such as: energy networks, water reservoirs, telecommunication system.

Terrorists have acknowledged the vulnerability of information networks and understood that, by destroying or altering communication networks, they may produce tensions with far more extended and dangerous effects than the old fashioned detonation of bombs in public places.

Therefore, *cyber-terrorism* is likely to become *the weapon of the powerful,* control of the information technology world will become the supreme weapon and the highest position will be attained by those who have information and initiate the attack.

We should not neglect the fact that *the more developed a country* is from the point of view of information technology, *the more vulnerable* will become and it will draw the attention of the perpetrators. Its strategic structures: telecommunications, energy systems, banking systems, health system, gas and petrol pipes will be the next targets of the enemies.

The more the world depends on the connections between essential services: commerce, finance, communications, transportation, energy, health, the more vulnerable we will be before terrorist cyber-attacks.

2.2. Cyber war – strategic war against informational era

Cyber war was defined by government expert Richard A. Clarke in his book, *Cyber War* (the first book about the war of the future – cyber war, the book is also a convincing argument that we are on the verge of losing such war unless we find efficient solutions to protect ourselves against cyber- attacks) as: "the action undertook by a nation-state to penetrate the computers or computing networks of another nation-state thus causing damage and malfunctions"[12].

It is said that the purpose of such cyber war is to affect and destroy critical infrastructures by using low cost means in order to generate a relevant impact on physical security, economic security, health and public safety.

Cyber war represents the means future wars will be fought. It is a war that does not involve significant costs but that may lead to immeasurable damage. During a cyber-war, we might face huge material damage, even casualties without even knowing who started the

[11] James Canton, *op. cit.*, 2010, p. 224.

[12] Richard A. Clarke, Robert K. Knake, *Războiul cibernetic: noua generaţie de ameninţări în securitate* (Cyber War: The Next Threat to National Security), ECCO Press, U.S., 2012.

attack. This represents a distinctive aspect in comparison to the classic and conventional war, a war we are familiar with, we know how it started and how it progresses. Another distinctive element is the need for cooperation between the public and the private sector so as to face such threats bearing in mind that intelligence services and the army have always been the tools of the state that used them in a sovereign and unilateral way[13].

The difference between *cyber war* and *cyber terrorism* resides in more motivation rather than mechanisms or effects. Understanding the distinction between these two offensive mechanisms is important in order to elaborate strategies, doctrines action and response tactics because, as the American futurist James Canton also asserted: "Cyber war is an asymmetrical war, a war with enemies that take multiple forms"[14].

2.3. Information technology espionage

- *Red October*. At the beginning of last year, the advanced network of cyber espionage, *Red October*, initiated an unprecedented attack against the national security of our country.

Kaspersky Lab, specialized in IT security products and services, released a research that identifies a very discrete espionage campaign aiming at targets from diplomatic, governmental and scientific fields of various countries.

The operation used viruses created so that it would enable access and copy files containing key words such as: *president, government, budget, European Union, United States*. The origin of the attack remains a mystery, especially because of the high number of sites that were attacked in very many countries.

The main objective of the perpetrators was to collect data and secret documents from the affected organizations in various countries, including geopolitical documents, access data to secured or classified networks, data from portable devices and network equipment.

It resulted from the investigations that the attackers concentrated on diplomatic and governmental agencies in various countries such as research institutions, energy companies including nuclear energy, commercial companies and aeronautic companies.

Romanian authorities reacted promptly and the spokesperson of the Romanian Intelligence Agency (the national authority in cyber-intelligence), Sorin Sava, stated[15] that the *Red October* cyber-attack mediatized by Kaspersky had been investigated by the agency ever since 2011 and the attack aimed at accessing IT networks of national interest and collecting "confidential information" but not classified information. Government institutions and embassies were attacked but their identity was not made public. *The cyber attacker aims at taking possession of documents regarding state policy and decisions taken by certain institutions*", the National Intelligence Agency sustains.

According to the National Centre of Response to IT Security Breaches (CERT-RO): "basing on the technical information we were provided with at the end of 2012 by Kaspersky Lab, we identified so far 4 IP addresses which were victims of Red October cyber-attack.

The authority sustains that it offered its support to ICI, the institute that handles RoTLD service in "identifying the causes of the security breach in order to determine the impact as well as the security measures that must be implemented to prevent further incidents"[16].

---

[13] Serghei Konoplyov, Iulian Fota, *Rusia nu va face niciun pas înapoi în privinţa scutului antirachetă*, in „Evenimentul Zilei" newspaper, 21 March, 2013, http://www.evz.ro/exclusiv-evz-geostrategul-serghei-konoplyov-rusia-nu-va-face-niciun-pas-inapoi-in-privin-10290.html.

[14] James Canton, *op. cit.*, 2010, p. 229.

[15] Sorin Sava, *SRI despre operaţiunea de atac cibernetic asupra României: octombrie Roşu*, în „Gândul" newspaper, 15 January 2013, http://www.gandul.info/stiri/sri-despre-operatiunea-de-atac-cibernetic-octombrie-rosu-asupra-romaniei-s-au-urmarit-informatii-confidentiale-nu-secrete-10468729.

[16] http://www.cert-ro.eu/articol.php?idarticol=701.

To this respect, the operations performed by the National Intelligence Agency point to the fact that the perpetrators has the necessary resources to value the retrieved data and take the initiative to launch further cyber-attacks against other institutions.

The conclusions of the authorities before the cyber-attacks that occurred in that last years are: "cyber threat represents one of the greatest and most dynamic threat to the national security of Romania and its allies; consequently, increasing the level of cyber security must become of priority for the Romanian state. Cyber security represents a dimension of the national security and the National Security Agency has the competence to deal with it; we have a good collaboration with other government institutions ad with private entities such as companies and universities"[17], is revealed in a press communication by the National Intelligence Agency.

- *MiniDuke.* Last year the cyber espionage attack by means of a malware program called *MiniDuke* was also oriented against Romania.

The specialists of the security company Kaspersky confirmed that many governmental institutions in various countries in Europe including Romania were spied on with a view to collecting confidential geopolitical data.

The attack was performed by using advance techniques consisting in sending PDF format documents towards the aimed targets; the documents in question were similar to those promoting a conference on the topic of human rights, Ukraine's foreign affairs strategy or NATO plans for the member countries. When the document was opened, the malware was installed on the computer and copied the desired information.

Kaspersky was the one that discovered the espionage operation and it stated that important information was compromised in countries such as Belgium, Ukraine, Romania, the Check Republic, Ireland, Portugal, a research center, two specialized organizations, a medical products supplier from the USA and a well-known research institute in Hungary.

The intensity of the attacks that occurred during the first two months of 2014 raised suspicions to Kaspersky experts; Eugene Kaspersky stated: "This is a very unusual cyber-attack. I remember this type of malware was used in the late '90s and the beginning of 2000. I wonder whether these programmers who had been inactive for more than a decade, suddenly awoke and joined a group of criminals who activate in the cyber world"[18].

According to the same source, the Romanian authorities admitted to the attack outlining that the cyber-attack called *MiniDuke* "*has a greater impact than Red October had because it had a superior technological level*". Moreover, it "was relevant in the area of Romanian national security and it was performed by an entity that bears the features of a nation actor".

According to the estimations of SRI specialists, this attack has the advantage of a better dissimulation with a view to retrieving information from the compromised network and upon examining the profile of the attacked institution, it was discovered that *it was meant to be an attack against national security*.

- *Epic Turla.* The cyber espionage operation called *Epic Turla*, aimed against our country in August 2014, was oriented against governmental institutions in Romania and our country was the most affected state because it occupied the first place in the world due to the number of infected sites, namely six. In our country the victims were ministries, governmental institutions, private companies or Internet users who access the Internet from governmental IP addresses.

[17] Sorin Sava, *op. cit.*, 15 January 2013.

[18] Eugene Kaspersky, *N-am mai văzut aşa ceva în ultimii 10 ani*, in „Gândul" newspaper, 27 February 2013, http://www.remembertoday.ro/articole-stiri/sursa/actualitate/Organizaii-guvernamentale-din-Europa-inclusiv-din-Romnia-victime-ale-unui-atac-informaticN-am-mai-vzut-aa-ceva-n-ultimii-10-ani-stire691033.html.

The ministries that were affected were: National Defense Ministry, Home Affairs Ministry, Foreign Affairs Ministry, as well as embassies and private companies that entered contracts with the above mentioned institutions, organizations that operate in the field of research and education, pharmaceutical companies.

These cyber-attacks "have as a source IT criminality networks, extremist-terrorist groups and even state actors", SRI spokesman declared[19].

Upon the examination of the source of the attacks, the specialists discovered a link between *Epic Turla* and *Miniduke* operations suggesting that the possible perpetrators speak Russian.

In July over one thousand companies located among which some were located in Romania, that develop operations in the energy field were infected with a sophisticated cyber virus thus the hackers gaining access to the control systems of energy plans; the main suspect was Russia.

Bearing in mind the latest global turmoil generated by Crimeea crisis, our country as NATO member, should focus its attention on protecting critical infrastructures since the threat to their integrity is permanent. Political analysts even stated: "long before green aliens and Russian tourists invaded Crimeea, Ukraine had been the victim of large scale cyber-attacks and so had Georgia and Estonia located at the center of NATO"[20].

If we wonder why Romania was and still is a potential target for cyber-attacks, Iulian Fota, the presidential counselor on security explains: "we were a target but we were not a victim because they did not succeed n affecting us badly. We have our own protection systems. Why did they attack us? This is something that must be clear to everyone: you cannot play in the Big League without drawing attention, animosity and adversity. While Romania is becoming a more and more relevant country at an international level, the focus of attention has started to span. We are member of NATO and UE and we will continue to be important to others. These may be individuals, organizations or even other states who wish to gain access to different information that we possess or even negatively influence certain activities or proceedings"[21].

Conclusions

Following increased cyber attacks on national critical infrastructures, developed in recent years, concrete measures have become a necessity, with a view to:

- increasing investment in IT security techniques aimed at maintaining safe systems able to provide critical infrastructure protection;
- training of specialists in network and data security with the purpose of timely identification and counteraction of computer system breaches;
- involvement of institutions, both public and private, tasked in the field of critical infrastructure in creating "a culture of data security" to raise awareness to the risks such entities are exposed to in cyber space;
- drafting of transparent, clearly defined methodological norms conducive to an effective implementation of the legislation in force in the area of cyber security and critical infrastructure protection.

[19] Sorin Sava, *Mai multe instituţii ale statului vizate de atacuri cibernetice*, în „Adevărul" newspaper, 7 August 2014, http://adevarul.ro/news/eveniment/sri-mai-multe-institutii-statului-vizate-atac-cibernetic-grupari-extremist-teroriste-1_53e3781e0d133766a81625da/index.html.

[20] Alexandru Georgescu, *Estul Europei, linia de front al unui război psihologic. Prinşi între Bidenology şi Kremlinologhie*, in „Economistul" Magazine, 19-26 May 2014, http://www.economistul.ro/estul-europei-linia-de-front-a-unui-razboi-psihologic-prinsi-intre-bidenology-si-kremlinologhie-a7115.

[21] Serghei Konoplyov, Iulian Fota, *op. cit.*, 21 March 2013.

The Supreme Council of National Defence of September 30, addressed issues relative to risks, threats and vulnerabilities forecast for Romania in 2015. Among them, types of cyber threats to national security and our country's response capacity to a major cyber attack, have triggered a response on the part of authorities; they have taken considerable steps in speeding up the enactment of the legal framework in the field of cyber security (see Cyber Security Law currently under debate in Parliament), the establishment of specialized bodies in evaluating national cyber security infrastructures, as well as measures aimed at school-level training in the area of cyber space security.

Acknowledgement:

This work was possible with the financial support of the Sectoral Operational Programme for Human Resources Development 2007-2013, co-financed by the European Social Fund, under the project number POSDRU/159/1.5/S/138822 with the title ***"Transnational network of integrated management of intelligent doctoral and postdoctoral research in the fields of Military Science, Security and Intelligence, Public order and National Security – Continuous formation programme for elite researchers - "SmartSPODAS"."***

BIBLIOGRAPHY:

1. CANTON James, *Future Challenges,* Polirom Publishing House, Bucharest, 2010.
2. Cristian Troncotă, et.al., *Insecurity Anxieties,* Tritonic Publishing House, Bucharest, 2005.
3. CLARKE A. Richard; Robert K. Knake, *Cyber War: The next threat to national Security and what to do about it,* ECCO Press Publishing House, U.S., 2012.
4. *National Defence Strategy 2010*.
5. GEORGESCU Alexandru, *Estul Europei, linia de front al unui război psihologic. Prinşi între Bidenology şi Kremlinologhie*, în Revista Economistul, 19-26 May 2014.
6. GOSTEV Alexander, *Cyberthreat Forecast for 2012*, 22 December 2011.
7. HURDUBAIE Ioan, *Atacurile cibernetice înlocuiesc terorismul ca primă ameninţare pentru Statele Unite ale Americii*, în ziarul Ultima oră, 25 March 2013.
8. KASPERSKY Eugene, *N-am mai văzut aşa ceva în ultimii 10 ani*, în ziarul Gândul, 27 February 2013.
9. KEMP R. Scott, *Cyberweapons: Bold steps in a digital darkness?,* in "The Bulletin of the Atomic Scientists", June 7, 2012".
10. KONOPLYOV Serghei, Iulian Fota, *Rusia nu va face niciun pas înapoi în privinţa scutului antirachetă*, în ziarul Evenimentul Zilei, 21 March, 2013.
11. LEE Dave, *Israel tops cyber-readiness poll but China lags behind*, in BBC News Technology, 30 January 2010.
12. MAIOR C. George, et.al., *A mind war - Intelligence, intelligence services and strategic knowledge in the 21st century,* RAO Publishing House, Bucharest, 2010.
13. SAVA Sorin, *SRI despre operaţiunea de atac cibernetic asupra României: octombrie Roşu*, în ziarul Gândul, 15 January 2013.
14. SAVA Sorin, *Mai multe instituţii ale statului vizate de atacuri cibernetice*, în ziarul Adevărul, 7 August 2014.

AN OPEN SOURCE ANALYSIS ON THE POTENTIALLY VOLATILE SECURITY ENVIRONMENT OF ASIA, A CASE STUDY OF SINO-INDIAN RELATIONS

Mihai Cătălin AVRAM
PhD. candidate, Faculty of Political Science, The University of Bucharest, member of Hans J. Morgenthau Centre and CIESPRISS (Interdisciplinary Centre for Excellence in Political Strategies, International Relations & Strategic Studies).

Abstract: *The study intends on exploring the actual and potential strains and tensions that may appear between India and China as they both strive towards gaining a central power status within Asia. The text will set off in analyzing open source intelligence in order to understand the nature of the military developments within the region while exploring the theoretical possibility of true full blown conflict between the two actors in the foreseeable future. Last but not least, the study will try to determine how third party states with interests in the Pacific Region, such as the United States of America, may react in order to contain, as much as possible, some of these developments in order to salvage the general security environment of the global arena.*

Keywords: *China, India, Japan, United States of America, naval power.*

Introduction

It is rather obvious that China is well on its way towards obtaining a global power status. As China has ascended, from an economical but also military point of view, it has managed to raise questions about global power balance, especially in the Asia-Pacific region. While seeking to cut some corners, in its effort to catch up with what Beijing is regarding as its most formidable enemy, the United States of America, China has set up a military project of billions of dollars, a apparently formidable cyber-force[1] and has been known to use classic forms of espionage, involving HUMINT collection methods[2], for the sake of boosting some high end military technologies. Before being fully capable of challenging the U.S. however, China has to be able to at least assume a superior power status within Asia, in regard to other possible future contenders to the status of regional leader. Naval powers in the area have understood this worrying trend and seem to react to it by pushing forward a containment agenda that would hinder Beijing in its efforts to expand its influence.

1. India-U.S. relations, a deterrent for China

China's official defence budget was 102.4 billion dollars in 2012.[3] This budget was increased to 119.5 billion dollars in 2014, "continuing more than two decades of sustained

[1] See for example *Exposing one of China's Cyber Espionage Units*, Mandiant, 2013.
[2] See for example the Noshir Gowadia case on open sources such as "US spy for China Noshir Gowadia jailed for 32 years", *BBC News*, 25.01.2011, http://www.bbc.co.uk/news/world-asia-pacific-12272941, consulted on 10.09.2014.
[3] International Institute for Strategic Studies, *the Military Balance 2013, the annual assessment of global military capabilities and defense economics*, p.41.

annual defence spending increases."[4] It is possible that Chinese defence spending add up to an overall bigger sum, since in 2013, according to the most pessimistic public evaluations made by United States' intelligence agencies, China had a defence budget that surpassed 215 billion dollars.[5] India has announced a defence budget of 38.35 billion dollars for 2014-2015[6] (3.1 times lower than China's). Both countries are dwarfed by the United States which spends about 645.7 billion dollars in 2012.[7]

The relatively small amount of resources spent by India in regard to defence is compensated by the fact that New Delhi and Washington have set out in a strategic partnership that could in theory activate their common military potential in case of any real need. The collaboration with the United States is thus for India a form of assurance that China cannot transform its complaints and adversities into a full military form. According to a report issued in 2011 by the Department of Defence of the U.S.A. "over the last decade the U.S.-India military relationship has known a rapid transformation. What has started as being an incipient relationship, between two states unfamiliar with one another, has transformed nowadays into a strategic partnership between two of the most prominent military powers of Asia. Today the military ties between the USA and India are strong and ever-more rising in intensity. The military relationship between the two countries embodies a vast array of domains such as military dialogue, military common exercises, military commerce as well as cooperation in the field of armament and exchange of experience."[8]

The signs of collaboration between India and the U.S. have become evident ever since George W. Bush was in office, when "according to the U.S.A. administration the most powerful democracy in the world and the most populous democracy in the world should collaborate"[9], probably, amongst other things, in order to introduce "a counterbalance to the rise of the Chinese power status."[10]

2. Measures of containment

India has not always used the American card in order to counteract the Chinese military build-up and has also been interested in increasing its power capabilities on its own. On the 20th of January 2004 Russia signed a contract with India by which Moscow obligated itself to provide New Delhi with a reconditioned aircraft carrier in 5 years time.[11] The 1.5 billion $ contract also envisaged the acquisition of several aircraft (29 fighters Mig-29K/KUB) and Russian helicopters that would populate the carrier.[12] After several delays, Admiral Gorshkov, now renamed INS Vikramaditya, (Brave as the Sun), has been officially

[4] *Annual Report to Congress Military and Security Developments Involving the People's Republic of China*, Office of the Secretary of Defense, 2014, p. 42.
[5] *Annual Report to Congress Military and Security Developments Involving the People's Republic of China*, Office of the Secretary of Defense, 2013, p. 45.
[6] Sanjee MIGLANI, "India raises military spending, eases foreign investment limit in arms industry", *Reuters*, 11.07.2014, http://in.reuters.com/article/2014/07/10/india-budget-defence-idINKBN0FF0WQ20140710, consulted on 10.09.2014.
[7] International Institute for Strategic Studies, *op. cit.* p.41.
[8] *Report to Congress on U.S–India Security Cooperation,* U.S Department of Defense, August 2013, p. 1.
[9] John FARDON, *India. Ascensiunea unei noi superputeri mondiale (India. The ascension of a new world superpower),* Bucharest, Litera Internaţional, 2008, p. 104.
[10] *Ibid.*
[11] Wade BOESE, "India buys Russian aircraft carrier", *Arms Control Association,* http://www.armscontrol.org/act/2004_03/India, consulted on 10.09.2014.
[12] "India buys Russia aircraft carrier", *CNN News*, 20.01.2004, http://articles.cnn.com/2004-01-20/world/india.warship_1_aircraft-carrier-india-admiral-gorshkov?_s=PM:WORLD, consulted on 10.09.2014.

commissioned to the Indian Navy.[13] This particular piece of information is important since the presence of any new such advanced weaponry within the Pacific alters the overall security balance of the area. Some might inquire into why India decided to buy an aircraft carrier from Russia since it has a very good partnership with the United States. The main reason is because the Russian carrier was cheaper. A Nimitz Class American airplane carrier costs 4.5 billion $[14], 3 times more than the Russian carrier set back the military expenditures of India.

India obviously decided to make such an investment as a response to reports of China's advancement in using carrier technology. China has bought a Kuznetsov class[15] airplane carrier from Ukraine in 1998[16] and after supposedly dissembling it, in order to understand its technology and enhance its capabilities, it fully commissioned it to the PLA in 2012.[17] It is true that the main target of the Chinese vessel did not seem to be India, since it had been stationed in Qingdao[18] and then to Yuchi Naval Base, located in the North See Fleet[19] (a lot closer to Japan, North and South Korea and also to Taiwan). However the Liaoning did perform local training exercises near Hainan islands in the South China Sea[20] which is a sign that the spam of the aircraft is not something to be taken lightly. Hainan is essential to Chinese strategic interests, as it became obvious in China's latest quarrels with most of its neighbours over Chinese sea influence. Recently an American P-8 Poseidon anti-submarine and reconnaissance plane has been intercepted in the area by a Chinese fighter demonstrating an aggressive attitude[21] which caused some diplomatic friction between the two countries.[22] All these demonstrate the importance of the South China Sea for Beijing and the fact that it has conflicting regional interests relatively close to the Bay of Bengal. Chinese officials have stated that China aims at building at least 2 new carriers in its military shipyards by 2022[23], which is obviously a worrying perspective for Indian officials and for American partners as well, since the balance of military power in the region is continuously being re-shaped by such developments.

---

[13] "PM Narendra Modi dedicates largest warship INS Vikramaditya to the nation, pitches for self-reliance", *The Indian Express*, 14.07.2014, http://indianexpress.com/article/india/india-others/prime-minister-narendra-modi-lands-on-indias-biggest-warship-ins-vikramaditya/, consulted on 10.09.2014.

[14] American Navy official Web page, http://www.navy.mil/navydata/fact_display.asp?cid=4200&tid=200&ct=4, consulted on 10.09.2014.

[15] *Annual Report to Congress Military and Security Developments Involving the People's Republic of China*, Office of the Secretary of Defense, 2013, p. 56.

[16] "US satellite snaps China's first aircraft carrier at sea", *The Guardian,* 15.12.2011, http://www.guardian.co.uk/world/2011/dec/15/us-satellite-china-aircraft-carrier, consulted on 10.09.2014.

[17] John REED, "China's carrier back at sea", *Defensetech*, 29.11.2011, http://defensetech.org/2011/11/29/photos-chinas-carrier-back-at-sea/, consulted on 10.09.2014.

[18] *Annual Report to Congress Military and Security Developments Involving the People's Republic of China*, Office of the Secretary of Defense, 2013, p. 73.

[19] *Annual Report to Congress Military and Security Developments Involving the People's Republic of China*, Office of the Secretary of Defense, 2014, p. 7.

[20] *Ibid.*

[21] David ALEXANDER, "U.S. protests intercept of Navy jet by Chinese warplane", *Reuters*, 23.08.2014, http://uk.reuters.com/article/2014/08/22/uk-usa-china-warplane-idUKKBN0GM1O520140822, consulted on 23.08.2014.

[22] Meghda RAJAGOPALAN, "U.S., China security leaders trade barbs over jet maneuvers", *Reuters,* 09.09.2014, http://news.yahoo.com/u-china-security-leaders-trade-barbs-over-jet-123648015--finance.html, consulted on 09.09.2014. For a fully detailed perspective you may also consult Mihai AVARAM, "Policy Brief No.24 : U.S. National Security Adviser Susan Rice visit to China: several hot topics discussed, with mixed results", *Hans J. Morgenthau Center,* 09.09.2014, http://morgenthaucenter.org/policy-brief-no-24-u-s-national-security-adviser-susan-rice-visit-to-china-several-hot-topics-discussed-with-mixed-results/.

[23] "China to build 2 more aircraft carriers: Taiwan" *Agence France-Presse*, 21.05.2012, http://www.defensenews.com/article/20120521/DEFREG03/305210003/China-Build-2-More-Aircraft-Carriers-Taiwan, consulted on 10.09.2014.

Besides being interested in performing modernization efforts by employing external technology, India is also pursuing the path of indigenous modernization. In this regard India has recently inaugurated INS Kolkata, a 6.800 ship, its biggest indigenous war vessel. The vessel is capable of reaching 30 knots (four gas turbines propulsion) and can fire 290 kilometre range BrahMos supersonic anti-ship cruise missiles.[24] INS Kolkata is viewed as a strategic asset that will "inspire confidence to those involved in maritime trade"[25] as the Prime Minister of India stated. But the deployment of such vessels is clearly a response mainly aimed at Beijing. Two new vessels, Kochi and Chennai, will supposedly follow the INS Kolkata at eight months intervals.[26]

India has also introduced to the navy INS Kamorta, an indigenously built 3.000 tons Anti-Submarine warfare Corvette,[27] probably as a response to Chinese increasing efforts of boosting its submarine capacity. Official sources note in this regard that "The PLA Navy places a high priority on the modernization of its submarine force. China continues the production of JIN-class nuclear-powered ballistic missile submarines (SSBNs). Three JIN-class SSBNs (Type 094) are currently operational, and up to five may enter service before China proceeds to its next generation SSBN (Type 096) over the next decade. […] The JIN-class and the JL-2 will give the PLA Navy its first credible sea-based nuclear deterrent. China also has expanded its force of nuclear-powered attack submarines (SSNs). Two SHANG-class SSNs (Type 093) are already in service, and China is building four improved variants of the SHANG-class SSN, which will replace the aging HAN-class SSNs (Type 091)."[28]

The Indian Kamorta took eight years to enter service, from the initial building phase and has shown some engine problems during its trail runs.[29] The ship is under the authority of the Eastern Ship Naval Command[30] a clear message to China's possible influence expansion agenda. However, some open sources note that "Kolkata and Kamorta have taken around a decade to roll out of the shipyards and the absence of key systems - Kolkata is without its main weapon, a long range surface-to-air missile system, while the submarine detecting towed array sonar is missing from both ships - has left a void even though the warships have been declared fully operational."[31] This puts India's indigenous modernization efforts under scrutiny and tends to underline lack of credibility.

---

[24] Akhilesh PILLALAMATTI, "India inaugurates largest indigenously built warship", *The Diplomat,* 20.08.2014, http://thediplomat.com/2014/08/india-inaugurates-largest-indigenously-built-warship/, consulted on 10.09.2014.

[25] *Ibid.*

[26] "India welcomes its first home-built warship: PM Modi commissions INS Kolkata as Defense Minister prepares launch of INS Kamorta", *Mail Online*, 16.08.2014, http://www.dailymail.co.uk/indiahome/indianews/article-2726840/India-welcomes-home-built-warship-PM-Modi-commissions-INS-Kolkata-Defence-Minister-prepares-launch-INS-Kamorta.html, consulted on 10.09.2014.

[27] "Frontline warship INS Kamorta commissioned", *The Times of India,* 23.08.2014, http://timesofindia.indiatimes.com/india/Frontline-warship-INS-Kamorta-commissioned/articleshow/40778412.cms, consulted on 10.09.2014.

[28] *Annual Report to Congress Military and Security Developments Involving the People's Republic of China*, Office of the Secretary of Defense, 2014, p. 8.

[29] "INS Kamorta: all you need to know about India's indigenous warship", *Daily News Analysis*, 23.08.2014, http://www.dnaindia.com/india/report-ins-kamorta-all-you-need-to-know-about-india-s-indigenous-warship-2013021, consulted on 10.09.2014.

[30] *Ibid.*

[31] "India welcomes its first home-built warship: PM Modi commissions INS Kolkata as Defense Minister prepares launch of INS Kamorta", *Mail Online*, 16.08.2014, http://www.dailymail.co.uk/indiahome/indianews/article-2726840/India-welcomes-home-built-warship-PM-Modi-commissions-INS-Kolkata-Defence-Minister-prepares-launch-INS-Kamorta.html, consulted on 10.09.2014.

India already has significant issues with projecting credible military naval power as shown in the past. On 14 August 2013, the INS Sinndhurakshak 10 Kilo-class Indian diesel-powered submarine exploded[32] while being stationed in the Lion Gate Mumbai dockyard for maintenance.[33] The vessel had previous problems in 2010 when an explosion at the battery compartment caused the Indian authorities to send the submarine to "The Zvezdochka shipyard in Russia for a two and a half year, 80 million$ retrofit. It was handed back to the Indian Navy in January, and went on a three month, 10.000 mile shakedown cruise that ended successfully in April in Mumbai."[34] This means one of two things. One might say that the submarine was not repaired correctly and it had a technical malfunction in 2013, either it was operated improperly. It makes no difference since both scenarios create an obvious problem for the Indian naval military forces. In the first scenario it means that India is operating faulty, unreliable, out of date military equipment, a theory that has been speculated upon by open sources that identify out of date Russian acquired equipment, including the MIG-21 fighters, to be one of India's problems in the long run.[35] In the second scenario, India is incapable of properly training its staff to operate military equipment. This would be an even more catastrophic image blow since the country has acquired on a lease a Russian Nerpa nuclear submarine for 10 years in 2012 for 1 billion $.[36] The mismanagement of such a vessel could pose bigger problems in the future.

3. The Japanese factor

For the U.S.A. the Chinese threat, in terms of shifting the power balance in the Pacific, would probably come by sea, which means that in order to assert its superiority, Washington must continue to find strategic partners at sea that are close to China and that can contain its influence area to a controlled environment. Such a partner is Japan which is known to have hosted the USS George Washington carrier vessel in Yokosuka in 2012.[37] More recently, on 25.08.2014, USS Hawaii, a 2 billion dollars Virginia Class nuclear powered submarine, docked at Yokosuka Naval Base in Japan. American Rear Admiral Stuart Munsch declared at that time that Americans were bringing their best to their "most important region"[38], a clear sign of efforts made to deter Chinese naval span and to empower a policy of containment.

Japan has also started to react to China's arms game and is apparently seeking to influence a lot more of the Pacific region in an effort to diminish potential Chinese naval influence. Such developments are linked to speculations regarding Australia's interest in buying diesel electric submarines from Japan.[39] Japan is also seeking to limit China's naval

---

[32] Yogita LIMAYE, "Indian submarine hit by explosion at Mumbai port", *BBC News Agency,* 14.08.2013, http://www.bbc.co.uk/news/world-asia-23691324, consulted on 10.09.2014.

[33] Gardiner HARRIS, "Grim hunt for 18 Indian Sailors Trapped on navy submarine after explosion", 14.08.2013, accessed 23 of August 2013 at http://www.nytimes.com/2013/08/15/world/asia/explosion-partly-sinks-indian-naval-submarine.html?ref=asia&_r=2&, consulted on 10.09.2014.

[34] *Ibid.*

[35] *Ibid.*

[36]Yogita LIMAYE, "Indian submarine hit by explosion at Mumbai port", *BBC News Agency,* 14.08.2013, http://www.bbc.co.uk/news/world-asia-23691324, consulted on 10.09.2014.

[37]Walter HICKEY, Robert JONSON, "These are the 20 aircraft carriers in service today", *Business Insider*, the 09.08.2012,http://www.businessinsider.com/the-20-in-service-aircraft-carriers-patrolling-the-world-today-2012-8?op=1, consulted on 10.09.2014.

[38] Anna FIFIELD, "With submarine, Navy tries to reassure friends in Asia - and warn foes", *The Washington Post*, 25.08.2014, http://www.washingtonpost.com/world/with-submarine-navy-tries-to-reassure-friends-in-asia--and-warn-foes/2014/08/24/8f683411-4b95-4676-990f-48cd552d5363_story.html, consulted on 10.09.2014.

[39] For a detailed analysis on this matter you may consult Ioana Corina JULAN, "Policy Brief No.23: Australia's new submarines – a strategic tool for 'containing' a growing China", ", *Hans J. Morgenthau Center*, 09.09.2014,

power status by tightening its relations to India directly. Recently, Prime Minister Shinzo Abe and Narendra Modi "said they would accelerate talks on the possible sale of an amphibious aircraft to India's navy."[40] Also, "the two prime ministers reaffirmed the importance of defence relations between Japan and India in their strategic partnership and decided to upgrade and strengthen them."[41] Overall open media states that "the deepening of defence relations has also raised hopes of a stronger maritime partnership. […] India and Japan could soon be in a strategic maritime embrace. "[42]

Conclusions

For now India is shield from any Chinese aggressiveness by a political, economic and military array of reasons. First of all, the Chinese would not risk a war in the Asia region because this would immediately alter its chances of continuing its economic efforts. "The military forces of the U.S. maintain a stable international order that has been decisively beneficial to the economic growth of China, and up until now Beijing has benefited from the security free of charge."[43] It will consequently not risk altering it, now more than ever, as the economic growth shows signs of stumble.[44] Moreover China is a very rational sovereign state and as such would not be willing to commit suicide since "many experts that have carefully studied the issue (of Chinese military growth in terms of power) agree on the fact that at this time China does not have the necessary military capacity in order to represent a threat to the United States within the Pacific region, although its modernization program has enhanced its capability of attacking the U.S.A. near the Chinese shoreline."[45] This means that although a defensive measure might be a potential possibility for Beijing, an offensive strike against the U.S.A. or any partnering country that the U.S.A. regards as of strategic importance, would be impossible.[46]

Even so, The United States is still at work in an effort to contain China's naval influence as much as possible. Japan, India and Australia are a key part of this strategy. As China's neighbours are constantly feeling the pressure from Beijing over its increasing naval sensibility, they too have decided to become closer military allies of the United States. Malaysia "has offered to host US Navy P-8A Poseidon aircraft (surveillance and anti-submarine) at a base on the edge of a disputed part of the South China Sea"[47], a move that is most likely linked to the strong position that China has in regard to its sensitive naval base in

---

http://morgenthaucenter.org/policy-brief-no-23-australias-new-submarines-a-strategic-tool-for-containing-a-growing-china/, consulted on 10.09.2014.

[40] "Japan-India move closer to boosting economic and defense ties", *The National*, 01.09.2014, http://www.thenational.ae/world/east-asia/japan-india-move-closer-to-boosting-economic-and-defence-ties, consulted on 10.09.2014.

[41] *Ibid.*

[42] Abhijit SINGH, "Rebalancing India's Maritime Posture in the Indo-Pacific", *The Diplomat*, 05.09.2014, http://thediplomat.com/2014/09/rebalancing-indias-maritime-posture-in-the-indo-pacific/, consulted on 10.09.2014.

[43] Robert D. KAPLAN, "The geography of Chinese power, how far can Beijing reach on land and at sea?", *Foreign Affairs*, Vol.89, No.3, May-June, 2010, p. 24.

[44] Kevin YAO, "China August factory growth slows to near six-year low, calls grow for more stimulus", *Reuters,* 13.09.2014, http://www.reuters.com/article/2014/09/13/us-china-economy-activity-idUSKBN0H803U20140913, consulted on 13.09.2014.

[45] Drew THOMPSON, "Regândiri. Armata Chinei. Nu e momentul să intrăm în panică. Încă." ("Rethinking the Chinese Army. It's not time to panic. Yet."), *Foreign Policy*, No. 15, March-April, 2010, p. 69.

[46] Robert D. KAPLAN, "The geography of Chinese power, how far can Beijing reach on land and at sea?", *Foreign Affairs*, Vol.89, No.3, May-June, 2010, p. 24.

[47] Trefor MOSS, "Malaysia offers to host U.S. navy aircraft", *The Wall Street Journal*, 12.09.2014, http://online.wsj.com/articles/malaysia-offers-to-host-u-s-navy-aircraft-military-official-says-1410524618, consulted on 12.09.2014.

Hainan. U.S. Navy Admiral Jonathan Greenert actually stated that Malaysia, Singapore and Indonesia are key to "the U.S. Navy successfully increasing its regional presence."[48] Indonesia is conducting military exercises with the United States, showing increasing ties between the two military structures. The most recent one was the eighth annual Garuda Shield exercise. During the opening ceremony, Lieutenant General Stephen Lanza, Commander of U.S. Army first Corps stated that "Bilateral exercises such as this one, broaden our knowledge and understanding of each other and build stronger bonds."[49]

Some American officials, such a Senator John McCain, do stress the fact that "India and the United States, two democratic great powers, can and should lead the 21st century in sustaining a liberal, rules-based international order, supported by a favorable balance of power."[50] This is a clear indicator to the fact that within the United States there are voices that see India as an important partner in balancing the power of China. Recent developments in regard to possible India-Japan ties tend to underline the common fear that both partners share in regard to Beijing's expansion agenda and Indian technological and naval responses to China's naval modernization programs are a clear sign that the Chinese threat is being addressed with due seriousness. However, New Delhi still needs to make its internal modernization effort more credible as the latest war ships to be unveiled have received criticism regarding improper equipment.

Acknowledgement:

This paper is made and published under the aegis of the Research Institute for Quality of Life, Romanian Academy as a part of programme co-funded by the European Union within the Operational Sectorial Programme for Human Resources Development through the project for Pluri and interdisciplinary in doctoral and post-doctoral programmes Project Code: POSDRU/159/1.5/S/141086
Sectoral Operational Programme Human Resources Development 2007-2013.
Project title: Pluri and interdisciplinary in doctoral and post-doctoral programmes
Editor of material:
Date of publication:

BIBLIOGRAPHY:

1. ALEXANDER, David, "U.S. protests intercept of Navy jet by Chinese warplane", *Reuters*, 23.08.2014, http://uk.reuters.com/article/2014/08/22/uk-usa-china-warplane-idUKKBN0GM1O520140822, consulted on 23.08.2014.
2. American Navy official Web page, http://www.navy.mil/navydata/fact_display.asp?cid=4200&tid=200&ct=4, consulted on 10.09.2014.
3. *Annual Report to Congress Military and Security Developments Involving the People's Republic of China*, Office of the Secretary of Defence, 2014.
4. *Annual Report to Congress Military and Security Developments Involving the People's Republic of China*, Office of the Secretary of Defence, 2013.

[48] *Ibid.*
[49] Brian C. ERICKSON, "Indonesia-U.S. exercise Garuda Shield begins in East Java", *Army.Mil*, 02.09.2014, http://www.army.mil/article/132892/Indonesian_U_S__exercise_Garuda_Shield_begins_in_East_Java/, consulted on 10.09.2014.
[50] "McCain's message to Obama, Modi: India, US can lead world in 21st century", *NITI Central*, 12.09.2014, http://www.niticentral.com/2014/09/11/mccains-message-to-obama-modi-india-us-can-lead-world-in-21st-century-237888.html, consulted on 13.09.2014.

5. BOESE, Wade, "India buys Russian aircraft carrier", *Arms Control Association,* http://www.armscontrol.org/act/2004_03/India, consulted on 10.09.2014.
6. FARDON, John, *India. Ascensiunea unei noi superputeri mondiale (India. The ascension of a new world superpower),* Bucharest, Litera Internaţional, 2008.
7. FIFIELD, Anna, "With submarine, Navy tries to reassure friends in Asia - and warn foes", *The Washington Post*, 25.08.2014, http://www.washingtonpost.com/world/with-submarine-navy-tries-to-reassure-friends-in-asia--and-warn-foes/2014/08/24/8f683411-4b95-4676-990f-48cd552d5363_story.html, consulted on 10.09.2014.
8. HARRIS, Gardiner, "Grim hunt for 18 Indian Sailors Trapped on navy submarine after explosion", 14.08.2013, accessed 23 of August 2013 at http://www.nytimes.com/2013/08/15/world/asia/explosion-partly-sinks-indian-naval-submarine.html?ref=asia&_r=2&, consulted on 10.09.2014.
9. HICKEY, Walter, JONSON, Robert, "These are the 20 aircraft carriers in service today", *Business Insider*, the 09.08.2012, http://www.businessinsider.com/the-20-in-service-aircraft-carriers-patrolling-the-world-today-2012-8?op=1, consulted on 10.09.2014.
10. International Institute for Strategic Studies, *the Military Balance 2013, the annual assessment of global military capabilities and defense economics*.
11. JULAN, Ioana Corina, "Policy Brief No.23: Australia's new submarines – a strategic tool for 'containing' a growing China", ", *Hans J. Morgenthau Center*, 09.09.2014, http://morgenthaucenter.org/policy-brief-no-23-australias-new-submarines-a-strategic-tool-for-containing-a-growing-china/, consulted on 10.09.2014.
12. KAPLAN, D. Robert, "The geography of Chinese power, how far can Beijing reach on land and at sea?", *Foreign Affairs*, Vol.89, No.3, May-June, 2010.
13. LIMAYE Yogita, "Indian submarine hit by explosion at Mumbai port", *BBC News Agency,* 14.08.2013, http://www.bbc.co.uk/news/world-asia-23691324, consulted on 10.09.2014.
14. MIGLANI, Sanjee, "India raises military spending, eases foreign investment limit in arms industry", *Reuters*, 11.07.2014, http://in.reuters.com/article/2014/07/10/india-budget-defence-idINKBN0FF0WQ20140710, consulted on 10.09.2014.
15. MOSS, Trefor, "Malaysia offers to host U.S. navy aircraft", *The Wall Street Journal*, 12.09.2014, http://online.wsj.com/articles/malaysia-offers-to-host-u-s-navy-aircraft-military-official-says-1410524618, consulted on 12.09.2014.
16. PILLALAMATTI, Akhilesh, "India inaugurates largest indigenously built warship", *The Diplomat,* 20.08.2014, http://thediplomat.com/2014/08/india-inaugurates-largest-indigenously-built-warship/, consulted on 10.09.2014.
17. RAJAGOPALAN, Meghda, "U.S., China security leaders trade barbs over jet maneuvers", *Reuters,* 09.09.2014, http://news.yahoo.com/u-china-security-leaders-trade-barbs-over-jet-123648015--finance.html, consulted on 09.09.2014..
18. REED, John, "China's carrier back at sea", *Defensetech*, 29.11.2011, http://defensetech.org/2011/11/29/photos-chinas-carrier-back-at-sea/, consulted on 10.09.2014.
19. *Report to Congress on U.S–India Security Cooperation,* U.S Department of Defense, August 2013.
20. SINGH, Abhijit, "Rebalancing India's Maritime Posture in the Indo-Pacific", *The Diplomat*, 05.09.2014, http://thediplomat.com/2014/09/rebalancing-indias-maritime-posture-in-the-indo-pacific/, consulted on 10.09.2014.

21. THOMPSON, Drew, "Regândiri. Armata Chinei. Nu e momentul să intrăm în panică. Încă." ("Rethinking the Chinese Army. It's not time to panic. Yet."), *Foreign Policy*, No. 15, March-April, 2010.
22. YAO, Kevin, "China August factory growth slows to near six-year low, calls grow for more stimulus", *Reuters,* 13.09.2014, http://www.reuters.com/article/2014/09/13/us-china-economy-activity-idUSKBN0H803U20140913, consulted on 13.09.2014.
23. "China to build 2 more aircraft carriers: Taiwan" *Agence France-Presse*, 21.05.2012, http://www.defensenews.com/article/20120521/DEFREG03/305210003/China-Build-2-More-Aircraft-Carriers-Taiwan, consulted on 10.09.2014.
24. "India buys Russia aircraft carrier", *CNN News*, 20.01.2004, http://articles.cnn.com/2004-01-20/world/india.warship_1_aircraft-carrier-india-admiral-gorshkov?_s=PM:WORLD, consulted on 10.09.2014.
25. "India welcomes its first home-built warship: PM Modi commissions INS Kolkata as Defense Minister prepares launch of INS Kamorta", *Mail Online*, 16.08.2014, http://www.dailymail.co.uk/indiahome/indianews/article-2726840/India-welcomes-home-built-warship-PM-Modi-commissions-INS-Kolkata-Defence-Minister-prepares-launch-INS-Kamorta.html, consulted on 10.09.2014.
26. "INS Kamorta: all you need to know about India's indigenous warship", *Daily News Analysis*, 23.08.2014, http://www.dnaindia.com/india/report-ins-kamorta-all-you-need-to-know-about-india-s-indigenous-warship-2013021, consulted on 10.09.2014.
27. "Japan-India move closer to boosting economic and defense ties", *The National*, 01.09.2014, http://www.thenational.ae/world/east-asia/japan-india-move-closer-to-boosting-economic-and-defence-ties, consulted on 10.09.2014.
28. "McCain's message to Obama, Modi: India, US can lead world in 21st century", *NITI Central*, 12.09.2014, http://www.niticentral.com/2014/09/11/mccains-message-to-obama-modi-india-us-can-lead-world-in-21st-century-237888.html, consulted on 13.09.2014.
29. "PM Narendra Modi dedicates largest warship INS Vikramaditya to the nation, pitches for self-reliance", *The Indian Express*, 14.07.2014, http://indianexpress.com/article/india/india-others/prime-minister-narendra-modi-lands-on-indias-biggest-warship-ins-vikramaditya/, consulted on 10.09.2014.
30. "US satellite snaps China's first aircraft carrier at sea", *The Guardian,* 15.12.2011, http://www.guardian.co.uk/world/2011/dec/15/us-satellite-china-aircraft-carrier, consulted on 10.09.2014.

AN OPEN SOURCE ANALYSIS REGARDING THE LATEST DEVELOPMENTS IN CHINA'S CYBERWARFARE AND ESPIONAGE STRATEGY

Mihai Cătălin AVRAM
PhD candidate, Faculty of Political Science, University of Bucharest; member of Hans J. Morgenthau Center and CIESPRISS (Interdisciplinary Center for Excellence in Political Strategies, International Relations & Strategic Studies).

Abstract: *It is clear that, for some time, the PLA has been mandated by Beijing to conduct several cyber espionage operations raging from hacking within private sector institutions, in the scope of getting a competitive advantage against adversaries, to obtaining intelligence from military and defence bodies. Some of these tactics have supposedly lead the way into the development of strategic assets, such as the Chengdu J-20, that will be used by Beijing in the effort of altering the power balance within the Asia Pacific area. It is therefore relevant to be up to date with latest developments regarding the cyber warfare and espionage issues that surround the Chinese power strategy. The study aims at understanding the latest Chinese developments in the fields of cyber warfare and espionage by examining open source data and strategic evaluations made by both private and official security bodies.*

Keywords: *cyber warfare, cyber espionage, USA, China, hacking, government, defence, industry.*

Introduction

It is clear that "cyberspace is America's operating system, analogous to a national-level Windows XP."[1] This is precisely why some actors, such as China have been using this as a weapon against the U.S. "Cyber warfare capabilities could serve Chinese military operations in three key areas. First and foremost, they allow data collection for intelligence and computer network attack purposes. Second, they can be employed to constrain an adversary's actions or slow response time by targeting network-based logistics, communications, and commercial activities. Third, they can serve as a force multiplier when coupled with kinetic attacks during times of crisis or conflict."[2] But as I will show this is a fairly narrow approach to the matter. The current paper thus studies the latest developments in the fields of Chinese cyber warfare and espionage, by using open source data and a broader definition linking the two elements together.

1. Definition of cyber warfare and espionage, a wider approach

Through cyber warfare some understand apocalyptic scenarios in which an actor is hit so hard via his network capacities that this disrupts his way of operating complex defensive structures, informational flux, usage of electric power on national level, and so on. Some see in cyber war the key to deterrence and associate it with a new sort of nuclear bomb. This is especially untrue in my opinion since ever since 2009 "Chong-Pin Lee, Vice Chairman of Taiwan's Mainland Affairs Council, said Beijing is re directing its emphasis away from

[1] Lt. Col. Scott W. BEIDLEMAN, "Defining and deterring Cyber War", *Strategy Research Project*, U.S. Army War College, Carlisle Barracks, 2009, pp. 1, 32.
[2] Office of the Secretary of Defense, *Annual Report to Congress, Military and Security Developments involving the People's Republic of China 2013*, Department of Defense, 2013, p. 36.

nuclear deterrence to this new asymmetrical strategy (cyber warfare)."[3] According to RAND specialists "cyber warfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks."[4] But all these perspectives are a bit narrow and do not put things into perspective.

The definition of cyber warfare that is both relevant for this study as well as for understanding Chinese cyber warfare and espionage tactics rests in research that was done a long time before networks even existed. It is derived from Clausewitz's famous observation linking war to politics. The author states: "We thus see that war is not only a political act, but a true political instrument, a continuation of political relations, a carrying out of politics by other means […] for the intention of politics is the aim, the war is the instrument and we can never see the instrument without the aim."[5] Thus war may be seen as being a continuation of political agendas trough other means. As we will see, cyber warfare is no different, as Beijing uses cyber instruments in order to continue its politics of shortening technological distances and competitiveness flaws. The general aim is to gain parity or closer to parity power to actors far superior to it, such as the United States. For China cyber warfare is merely a new way of augmenting its military and economic power, a continuation of its politics trough means that are associated with areas such as the Internet, networking etc.

This understanding of warfare, starting from the thinking patterns associated with Clausewitz, allows us to understand cyber espionage not as a separate phenomenon but rather as a subordinated instrument used within the larger cyber war framework. Espionage is mainly aimed at attaining information, regardless of the field in which it is conducted. "Trough information we designate all knowledge that we have attained in regard to the enemy and its country, that is to say the basis of all our ideas and actions. Let us consider the nature of this basis, with its dubious and unstable character, and we will soon see how dangerous the whole edifice of war is and how easily it can crumble, burying us under the debris."[6] Cyber espionage makes the edifice stronger, by providing more and more data and by helping the source of the cyber activity understand his enemy better and devise strategies against him. Thus we understand that cyber espionage is not a separate field in this regard but merely an instrument that is subordinated to the bigger prospects of war and cyber war. It comes to fill in the gap in knowledge and thus resolves a problem as old as time, that of allowing us to do sufficient calculus in order to be fully informed upon acting. "By doing more calculus winning becomes possible; if we do less, victory is impossible. How much the chances are reduced for he who does no calculus whatsoever!"[7] Cyber espionage allows calculus to be made and extends the reach of political and national agendas far beyond their classical power capacities. This is why I will be tempted to treat cyber war and cyber espionage not as separate fields, but as elements that are woven together generating an asymmetric instrument of power used by Beijing in its developing power strategy.

Thus we arrive at the explanation the cyber warfare is a continuation of Beijing's political agenda and that cyber espionage is merely an instrument used as part of this agenda projection onto the world.

---

[3] Gurmeet KANWAL, "China's Emerging Cyber War Doctrine", *Journal of Defense Studies,* Vol. 3, No. 3, July, 2009, pp. 15, 22.
[4] "Cyber warfare", *RAND*, http://www.rand.org/topics/cyber-warfare.html, consulted on September 6, 2014.
[5] Carl Von CLAUSEWITZ, *Despre Război (On War)*, Editura Militară (Military publishing house), Bucharest, 1982, p. 67.
[6] *Ibid.,* p. 102.
[7] Sun TZU, *Arta Războiului (The Art of War),* Antet XX, Bucharest, ISBN 973-96045-6-0, p. 15.

2. Overview

As Chinese power became more prominent, a result of an expanding economy and a rise in military power, experts have noted that Beijing shifted its obsessive attention on Taiwan towards a wider regional defence plan.[8] It is obvious, just by locking at latest developments, that the increase in Chinese military naval power and the increase of its perceived influence have caused China to enter territorial disputes with a fair number of its neighbours. As part of this expansion strategy, with world-wide implications, China has introduced some modernization efforts to its cyber capabilities. "This modernization effort known as informatization is guided by the doctrine of fighting *Local War under Informationized Conditions* which refers to the PLA's ongoing effort to develop a fully networked architecture capable of coordinating military operations on land, in air, at sea, in space and across the electromagnetic spectrum."[9]

This trend has been analyzed by a number of sources, especially in the U.S. As we have noted in the introduction of this paper the U.S. heavily relies on cyber know-how and infrastructure in order to coordinate a large amount of information and activity critical to national power and strategy. Thus, the U.S. currently follows with great tenacity ongoing developments in the field. The latest report on Chinese military preparedness issued by the Department of Defence thus states that "Beijing is investing in military programs and weapons designed to improve extended-range power projection and operations in emerging domains such as cyber, space, and electronic warfare."[10] There is consequently open source data proving that Beijing is developing its cyber abilities in the military field. As we will see, civilian use of cyber instruments is just as important and Beijing frequently uses cyber tactics in order to augment its capacities in economy, industry and international relations.

As a general truth we may observe that "in 2012, numerous computer systems around the world, including those owned by the U.S. government, continued to be targeted for intrusions, some of which appear to be attributable directly to the Chinese government and military. These intrusions were focused on *exfiltrating* information. China is using its computer network exploitation (CNE) capability to support intelligence collection against the U.S. diplomatic, economic, and defence industrial base sectors that support U.S. national defence programs. The information targeted could potentially be used to benefit China's defence industry, high technology industries, policymaker interest in US leadership thinking on key China issues, and military planners building a picture of U.S. network defence networks, logistics, and related military capabilities that could be exploited during a crisis. Although this alone is a serious concern, the accesses and skills required for these intrusions are similar to those necessary to conduct computer network attacks. China's 2010 Defence White Paper notes China's own concern over foreign cyber warfare efforts and highlighted the importance of cyber-security in China's national defence."[11] The fact that espionage necessitates intrusion signifies that the sovereign actor that is fluent in extraction techniques may very well be prepared in activities that would aim at destroying or inhibiting the normal functionality of say a defence network system or a strategic infrastructure segment.

Chinese efforts in conducting such operations are obvious. "In late February 2014, China announced a new Central Internet Security and Informatization Leading Group. President Xi Jinping chairs the leading group, reflecting the importance Beijing ascribes to the

[8] Bryan KREKEL, George BAKOS, Christopher BARNETT, "Capability of the People's Republic of China to conduct Cyber Warfare and Computer Network Exploitation", *The US-China Economic and Security Review Commission*, 2009, p. 6.
[9] *Ibid.*
[10] Office of the Secretary of Defense, *op. cit.*, p. 29.
[11] *Ibid.*, p. 36.

issue. Leading groups are deliberative committees at the top levels of the CCP that influence policy through their coordinating function and recommendations to the Politburo Standing Committee, the top-level decision-making body in China."[12] We may thus observe that cyber activities abroad can and are being linked with the politburo agenda which signifies that the line between military, commercial and diplomatic use of cyber warfare and espionage techniques is dim to say the least. We have known for some time that many of these actions may be linked to the PLA[13] since China has previously announced that it had set out what we know today as "The Blue Team", a team of PLA operatives (supposedly 30 in the beginning) that operate in the field of cyber activities, for defensive purposes, according to the PLA.[14]

Expansion of interests and reach

The US-China Economic and Security Review Commission issued a paper in 2009 underlining security threats associated with China's cyber warfare capabilities. The document included an index of the most notorious cyber attacks believed to have originated from China.[15] The index was composed of open source intelligence regarding the issue from 1999 until 2009. Upon consulting the different events I have observed the following. 31 events have been registered as being traced directly to China. Eight of these events regarded malicious cyber activities against Taiwan, 11 against the United States, one against Japan, two against Germany, two against the United Kingdom, one against New Zeeland, one against India, one against Belgium, one against France, one against Australia and one against South Korea. One event concerned 103 states. The attacks have certainly been more numerous but these are just instances in which open sources firmly reacted.

Out of all mentioned attacks, four have been linked to revenge purposes (a reaction of underground hackers trying to take revenge on France for associating with the Dalai Lama or actions taking revenge on Taiwan for obvious reasons). 15 events included actions aimed at undermining websites of government facilities and acquiring data from foreign governments. Six of the events included efforts to obtain data or disturb activities in the economic or financial private sector. Seven of the events regarded disrupting, spying on or hacking for other reasons into systems associated with military technology, planning and strategizing. Sources linked to China hacked into a nuclear facility on U.S. soil at least once and into space related technology facilities (NASA) once more. On one event an academic facility was hacked. The very short study shows that China mainly used social engineered emails in order to gain access to information. It also demonstrates that, as time goes by, Chinese interests are expanding from the regional to the global level as hacking is no longer constantly associated with Taiwan (as it was until 2004).

It also demonstrates that there is a shift from merely blocking official sites to acquiring sensitive military, economic or government strategy data.

Although some of the events did seem to have a revenge factor (lacked a coordinated strategy and merely tried to undermine the credibility of official web-sites), most of the activities regarded blocking or gathering information from different branches of government activities. An attack on the Pentagon of 20 terra worth of information and the one on 103 states are the most obvious examples of both Chinese interests for sensitive data as well as

[12] Kimberly HSU, Craig MURRAY, *China and International Law in Cyberspace*, U.S. - China Economic and Security Review Commission Staff Report, may, 6, 2014, p. 5.
[13] Abbreviation for People's Liberation Army.
[14] "China Conforms Existence of Elite Cyber-Warfare outfit the *blue Army*", *Fox News*, 26.05.2014, http://www.foxnews.com/tech/2011/05/26/china-confirms-existence-blue-army-elite-cyber-warfare-outfit/, consulted on September 6, 2014.
[15] The following short study is based on data (from Bryan KREKEL, George BAKOS, Christopher BARNETT, *op. cit.*, pp. 68; 74) which I have processed into categories of interest.

ability to attain global reach.[16] Operation "Shady RAT" of 2011, targeting companies, governments and NGO's in at least 14 states demonstrates the extent of the reach and know-how that have been linked (without auxiliary proof) to Chinese international cyber interests in the fields of government, industry, aerospace, defence, financial sector, academic and NGO.[17]

3. Unit 61398

The most recent document, and the first, which actually has assumed the responsibility of linking cyber-espionage activities to a military unit within China has been provided by Mandiant, an information security company specialized in informational breach identification and assessment of breach impact on the client. In February 2013 Mandiant's Threat Intelligence Centre developed a report in which it stated that it had positively identified PLA Unit 61398 as a cyber espionage unit specialized in the theft of documentation raging in a vast domain field. The unit is based in Pudong New Area of Shanghai and has been evaluated by Mandiant starting from 2006. During this time Mandiant states that APT1[18] managed to compromise 141 companies in 20 major industry fields. It seems that at some point the threat remained connected to a victim for four years and eight months and managed to steal 6.5 terabytes worth of information from a single organization in only 10 months.[19] Among the data that helped link APT1 to PLA Unit 61398 where: the location from which the attack was proliferated (overlapping the area where the unit is stationed), the requirements for personnel that composed the unit (network skills and fluent English), the strategic importance (supported by China Telecom by being provided full fiber optic communication infrastructure in the name of national defence), the targets that APT 1 was interested in (industries labeled as strategic by Beijing), the usage of Chinese language for some of the programming tools used to hack and so on.[20] After assessing a considerable volume of information Mandiant concludes that "the sheer scale and duration of sustained attacks against such a wide set of industries from a singularly identified group based in China leaves little doubt about the organization behind APT1. We believe the totality of the evidence we provide in this document bolsters the claim that APT1 is Unit 61398. However, we admit there is one other unlikely possibility: A secret, resourced organization full of mainland Chinese speakers with direct access to Shanghai-based telecommunications infrastructure is engaged in a multi-year, enterprise scale computer espionage campaign right outside of Unit 61398's gates, performing tasks similar to Unit 61398's known mission."[21]

PLA Unit 61398 areas of interest are the US, Canada and other English speaking areas. Its main aim is to obtain political, economic and military intelligence.[22] The number of attacks proliferated by the agency rose consistently from 2007 to 2013 according to a chart made available by Mandiant. The Mandiant team was also able to identify a certain Jack

[16] Due to a lack of space I have decided not to introduce a table in which to make this data more viewer-friendly. I also have to note that there may be differences between the overall number of attacks mentioned and the overall number of attacks mentioned per field of interest (i.e. government, military and so on). This is because some attacks have multiple purposes in multiple fields which I have counted separately. This is also why I have decided not to use percentage points in order to show a relative statistical activity for the fields of interest because they would have not made sense to the reader.
[17] Dmitri ALPEROVITCH, "Revealed: Operation Shady RAT", *McAfee Threat Research White Paper*, 2011, pp. 1; 14.
[18] Abbreviation derived from Advanced Persistent Threat. ATP1 was identified as being PLA Unit 61398 by Mandiant.
[19] *Exposing one of China's Cyber Espionage Units*, Mandiant, 2013, pp. 1; 3.
[20] *Ibid.*, pp. 3; 4.
[21] *Ibid.*, p. 6.
[22] *Ibid.*, p. 7.

Wang/ Wang Dong, a.k.a. *ugly gorilla* as one of the persons involved in acts of espionage.[23] Wang had previously used a public forum to get in touch with a professor in China, retired Admiral Zhang Zhaozhong, who was an advocate of military informatization.[24] Although many forms of hacking are performed in order to gather sensitive data, *Spear Phishing Emails* still remains one of them, as in the case of the observed 1999-2009 trends. Ever since 2009 experts noted that there is "increasing evidence that the intruders are turning to Chinese black hat programmers (i.e. individuals who support illegal hacking activities) for customized tools that exploit vulnerabilities in software that vendors have not yet discovered. […] Although these relationships do not prove any government affiliation, it suggests that the individuals participating in ongoing penetrations of US networks have Chinese language skills and have well established ties with the underground Chinese hacker's community. Alternatively, it may imply that the individuals targeting US networks have access to a well resourced infrastructure that is able to broker these relationships with the Chinese black hat hacker community and provide tool development support often while an operation is underway."[25] This is why we are tempted to believe that "a high-priority for China's advanced technology acquisition strategy is its Civil-Military Integration policy to develop an innovative dual-use technology and industrial base that serve both military and civilian requirements. China's defence industry has benefited from integration with its expanding civilian economy and science and technology sectors, particularly sectors with access to foreign technology. Examples of technologies include: advanced aviation and aerospace (hot section technologies, avionics and flight controls), source code, travelling wave tubes, night vision devices, monolithic microwave integrated circuits, and information and cyber technologies."[26] Recruiting black hats such as *ugly gorilla* may be a strategy. Using them without introducing them into military infrastructure might also be an idea since this would allow China to deny responsibility. Nevertheless interest fields and general domains targeted seem to imply government interests.

What is ever more worrying is that "some aspects of cyber war are indistinguishable from the kinds of cyber attacks designed to inflict catastrophic destruction. For example, efforts to penetrate a computer system for the purpose of exfiltrating data are often indistinguishable from efforts to penetrate a system for the purpose of planting a logic bomb or executing a cyber attack (e.g., corrupting or deleting data, compromising a control system). This may make it difficult and perhaps impossible to discern promptly when a rival has transitioned from acts of cyber espionage, crime, and economic warfare to an attack on its adversary's critical infrastructure."[27] This also means that Unit 61398 may be on a learning curve which allows it to both extract essential data as well as to understand sophisticated government and private cyber infrastructure and fire-walling techniques, a activity that might come in handy in case of the breakout of a full scale cyber war.

United States' response

Well before cyber warfare and cyber espionage became hot topics in international discussions, "in 1997, the U.S. military conducted Eligible Receiver, the nation's first-ever information warfare exercise. This exercise tasked a group of highly trained, computer experts, known as a government red team, to independently examine plans and operations from the perspective of adversaries. The red team was able to infiltrate and take control of

[23] *Ibid.*, pp. 52, 55.
[24] *Ibid.*, pp. 52.
[25] Bryan KREKEL, George BAKOS, Christopher BARNETT, *op. cit.*, pp. 6, 7.
[26] Office of the Secretary of Defense, *op. cit.*, p. 12.
[27] Andrew F. KREPINEVICH, *Cyber Warfare, a nuclear option?,* Center for Strategic and Budgetary Assessment, 2012, p. 68.

Pacific command center computers, as well as power grids and 911 systems in nine major U.S. cities. These results suggested that America's critical military and civilian infrastructures were highly vulnerable. In fact, the very next year hackers confirmed the findings of Eligible Receiver when they attacked Department of Defence networks and compromised over 500 computers in the incident dubbed *Solar Sunrise.* This attack targeted logistics and accounting systems essential to managing and deploying U.S. military forces at a time when the U.S. was considering military action against Iraq for failing to comply with UN resolutions."[28] The U.S.A. is well aware of its flaws and vulnerabilities in the cyber field and several actions have thus been taken in order to secure networks of strategic value. We may also assume the fact that since Mandiant, a private contractor, was able to track Chinese movements on the cyber espionage front for quite a long time, U.S. specialized segments of the military and intelligence can do the same. This implies that the United States, although a target for cyber activities, may very well follow and understand better and better the tactics used by Chinese sources in order to infiltrate targets. This knowledge helps secure networks and attain know-how in blocking protocols.

Usually "China publicly portrays its cyber-related military capabilities as a defensive response to what it views as *hegemonic* efforts by the United States to militarize cyberspace with offensive capabilities. In their writings, PLA academics consider a multidimensional information warfare environment more complex than a binary offense-defence scenario in cyberspace. However, China publicly portrays U.S. cyber policies as indicative of offensive U.S. intentions in cyberspace requiring China's defensive response."[29] However, open source suggests that the United States are ever more often able to pin-point more accurately the source of actual Chinese cyber attacks. An indicator to this is the law suit that the U.S. government has started against Sun Kailiang, Huang Zhenyu, Wen Xinyu, Wang Dong and Gu Chunhui for activities of cyber espionage. All of the men are part of the PLA and are working with PLA Unit 61398.[30] Wang Dong (*ugly gorilla*) was identified by the Mandiant report as one of the most prolific hackers working for the Unit.[31] The 2014 accusations are linked to cyber activities regarding theft of nuclear, metal and solar panel information from private companies within the U.S.[32] The law suit is an indicator to the fact that Washington is no longer willing to keep a relative silence in regard to Chinese cyber actions as well as an indicator to the fact that the United States takes its private sector security very seriously. The law suit also demonstrates that intelligence services are linking cyber espionage to the PLA. It shows that military and commercial interests in China are being blurred out since PLA operatives hack into private sectors abroad

Conclusion

Some sources note that "cyber war appears to have even less basis for a strategic treatment than space warfare or electronic warfare. Its efficacy—much less significance—has been postulated well before it has been proven."[33] This is to say that even if the threats associated with cyber warfare are numerous we have yet to see a scenario in which apocalyptic cyber developments have been proven. Nevertheless this view is dependent on the

[28] Lt. Col. Scott w. BEIDLEMAN, *op cit*.
[29] Kimberly HSU, Craig MURRAY, *op. cit.*, p. 1.
[30] Sui-Lee WEE, "China confronts U.S. envoy over cyber-spying accusations", *Reuters,* 10.05.2014, http://www.reuters.com/article/2014/05/20/us-china-usa-espionage-idUSBREA4J03D20140520, consulted on September 6.2014.
[31] *Exposing one of China's Cyber Espionage Units*, *op.cit.*, pp. 55.
[32] Sui-Lee WEE, *op. cit.*
[33] Martin C. LIBICKI, "Why Cyber War will not and should not have its grand strategist", *Strategic Studies Quarterly*, spring, 2014, pp. 23; 39.

approach we have on defining war. I consider that the open source data delivered as part of this paper suggests that cyber warfare and espionage are linked since they are both associated with the military and Chinese government. Latest developments suggest that a border between state and private interest cannot exist in China which leads us to believe that most hostile Chinese cyber activity is only a continuation of Beijing's policy. This offers us sufficient grounds in order to state that China is conducting cyber war activities currently since war may be defined as a continuation of politics through other means.

The paper embraces the long term perspective described by "IISS[34] Director-General and Chief Executive John Chipman (who) recently said that *future state-on-state conflict may be characterized by the use of so called asymmetric techniques. Chief among these may be the use of cyber-warfare.*"[35] But even if states will have to advance cyber warfare capabilities "in order to be able to attack and paralyze an adversary's military capacity or the adversary's ability to control its own forces"[36] such perspectives are only viewing half of the problem as I have shown that Chinese cyber abilities in espionage can be viewed as part of its efforts to destabilize states by using instruments of destruction and acquisition of information in the private sector. This is just as worrying as the military perspective since such fields of private industry are intricately linked to elements of national power.[37] By hitting government, military and industry, Chinese cyber efforts present a continuation of Chinese political interests abroad, in fields that have the potential of shortening the power distance between Washington and Beijing. China will probably continue to use the PLA in order crack sophisticated cyber infrastructures in its efforts of getting competitive advantages and technological parity with strong power structures such as the U.S.

Acknowledgement:

This paper is made and published under the aegis of the Research Institute for Quality of Life, Romanian Academy as a part of programme co-funded by the European Union within the Operational Sectorial Programme for Human Resources Development through the project for Pluri and interdisciplinary in doctoral and post-doctoral programmes Project Code: POSDRU/159/1.5/S/141086
Sectoral Operational Programme Human Resources Development 2007-2013.
Project title: Pluri and interdisciplinary in doctoral and post-doctoral programmes
Editor of material:
Date of publication:

BIBLIOGRAPHY:

1. ALPEROVITCH, Dmitri, "Revealed: Operation Shady RAT", *McAfee Threat Research White Paper*, 2011.
2. CLAUSEWITZ, Von Carl, *Despre Război (On War)*, Editura Militară (Military publishing house), Bucharest, 1982.
3. HSU, Kimberly; MURRAY, Craig, *China and International Law in Cyberspace*, U.S. - China Economic and Security Review Commission Staff Report, may, 6, 2014.

[34] Abbreviation for International Institute for Strategic studies.
[35] Magnus HJORTDAL, *op.cit.*
[36] *Ibid.*
[37] As seen by the Classical Realist Paradigm associated with Hans J. Morgenthau. See Hans J. MORGENTHAU, *Politics among nations, the struggle for power and peace,* Alfred A. Knopf, New York, 1948, pp. 80; 109 where the author discusses elements of national power and includes within these items factors such as "Industrial Capacity" (pp. 86; 88), "Military Preparedness" (pp. 88; 91) and "Quality if Diplomacy" (pp. 105; 109).

4. KANWAL, Gurmeet, "China's Emerging Cyber War Doctrine", *Journal of Defence Studies,* Vol. 3, No. 3, July, 2009, pp. 15; 22.
5. KREKEL, Bryan; BAKOS, George, Christopher BARNETT, "Capability of the People's Republic of China to conduct Cyber Warfare and Computer Network Exploitation", *The US-China Economic and Security Review Commission*, 2009.
6. MORGENTHAU, J. Hans, *Politics among nations, the struggle for power and peace,* Alfred A. Knopf, New York, 1948.
7. TZU, Sun, *Arta Războiului (The Art of War),* Antet XX, Bucharest, ISBN 973-96045-6-0.
8. Office of the Secretary of Defence, *Annual Report to Congress, Military and Security Developments involving the People's Republic of China 2013*, Department of Defence, 2013.
9. Mandiant, *Exposing one of China's Cyber Espionage Units*, 2013.

INDEX

"CAROL I" NATIONAL DEFENCE UNIVERSITY PUBLISHING HOUSE

Director: Colonel Alexandru STOICA, PhD Lecturer

"Carol I" National Defence University Printing House
Panduri Street, no. 68-72, sector 5, Bucureşti
e-mail editura@unap.ro
Tel: 021/319.40.80/453
Fax: 021/319.59.69

932/2014 C. 279/2014