„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

THE COMPLEX AND DYNAMIC NATURE OF THE SECURITY ENVIRONMENT

Volume 2

Editors
Stan ANTON
Iuliana SimonaȚUȚUIANU

June 11-12, 2015
Bucharest - Romania

ISSN 2285-9896
ISSN-L 2285-8318

CONTENTS

MILITARY GEOGRAPHY – PRECURSOR OF GEOSTRATEGY

Silviu NEGUŢ, PhD
Professor, Bucharest University of Economic Studies
silviu.negut@gmail.com

Abstract: *Geostrategy as a concept, although older than the geopolitics concept, was rarely used due to terminological confusions and, moreover, because of the existence of Strategy and Military geography as well individualized disciplines. This study demonstrates that Military geography, a discipline more complex than it seems, is the true precursor of Geostrategy.*

Keywords: *Geostrategy, Geography, Military geography, Strategy, Geopolitics*

Preliminaries or the beginnings of *Geostrategy*

As in *Geopolitics*, the phenomenon that characterize *Geostrategy* are much older than the time of its concretization as the concept that we now today. There has always been a territorial stake, a certain configuration of the scene of operations, exploited by the „actor" who knew her best. This (territorial stake) is, as pointed out by an expert in this field, "a constant which is found in all historical periods and who continues to make its effects felt despite the prodigious development of communication means."[1]

As will be showed, there is a close link between *Geopolitics* and *Geostrategy*, sometimes the two terms becoming synonymous. However, if in the first case, the year in which the concept was mentioned as terminology was very clear (in 1899, by Rudolf Kjellén a Swedish politician in a conference), in the second case, confusion existed for a long time. The idea that it is a fairly recent development was contradicted only a short while ago, establishing the origins of Geostrategy to be more the 50 years prior to the first term presented, in 1846, being used by the italian Giacomo Della Durando in his work *Della nazionalita italiana*. He makes surprising appreciations for those times and besides the *geostrategy* concept inserts the *geotactics* concept too:

"I used a word that I do not think has been used until now, *geostrategy* (emphasis added), whenever it was necessary to appreciate the land as an abstract concept and outside of using organized forces, but, naturally always in relation to them. Therefore, I speak in both *geostrategic* and *geotactical* (emphasis added) *terms* of Italy and Spain, when I am studying the abstract structure and characteristics of the land, but I speak about movements or strategic or tactical axis operations when it comes to military operations carried on some fixed points of land. Therefore I separate, by reasoning and for greater clarity these two ideas which, are never mutually exclusive in both theory and practice."[2]

Unfortunately, the two terms have not taken roots: one (*geotactics*) disappeared into nothing, and the other (*geostrategy*) returned to public attention much later. In the latter case it did not have an effect either the iberian studies of some analysts that, as Durando, included in the title of their work the concept: *Estudo geoestratégico de Portugal* (1890, spanish Colonel Manuel Castaños y Montijano) and *Estudio geo-éstrategico dos teatros de operações nacionais* (1932, portuguese Colonel Miranda Cabral). The explanation is that in those times the *Military geography* was more spectacular.

[1] Hervé Coutau-Bégarie (2008), *Traité de Géostratégie*, 6eme edition, Editions Economica, Paris, p. 759.
[2] Apud Ferrnicio Botti (1995), *Le concept de géostratégie et son application la nation italienne dans les théories du géneral Durando*, în „Stratégique", 58, 1995-2, p. 129.

Some analysts consider that the man who founded the modern geostrategy is the american geopolitician with dutch origins Nycholas Spykman which, in his *America's Strategy in World Politics* work (1942), makes a real geostrategic analysis of the Western Hemisphere and in *The Geography of the Peace*, published posthumously (in 1944, a year after his death), defines the very essence of geostrategy: "In time of global warfare, military strategy must consider the whole world as a unit and to consider all fronts as there are in their mutual relations"[3].

But he does not use the *geostrategy* word, although there are implicit references. In fact neither do other analysts who have similar merits, such as americans Hans W. Weigert and Vilhjalmur Stefansson (*Compass of the World*, 1944), french Amiral Raoul Castex (*Théories stratégiques*, 1929-1939), Czechs Fritz-Otto Miksche (*Les erreurs stratégiques de Hitler*, 1945; *War Between Continents*, 1948) and Emanuel Moravec (*La Stratégie nouvelle*,1941) and others.

The merit of "reinvention" of the *geostrategy* term, almost 100 years after was mentioned by the italian Giacomo Durando, rests with the american George B. Cressey, with a paper published in 1944, in which he sustains that geostrategy is opposite from militaristic and imperialistic geostrategy: "Geostrategy's function is to understand the problems and the potential of a nation and to suggest an internal development and international cooperation program for everyone's welfare"[4]. Others that supported this vision were spaniard Kindelan (*Geobelica*, 1945), the french Camille Rougeron (*La Prochaine guerre*, 1948) and Pierre Célérier (Géopolitique *et géostratégie*, 1955), the Brazilian Galbery do Cunto e Silva (*Geopolítica e geoestrategia*, 1959), the american Saul B. Cohen (Geography and Politics *in a World Divided*, 1963), the argentine Justo P. Briano (*Geopolítica et geostrategia americana*, 1966). But there was little work for a period if several decades. Only with the 70^{s}, their number has multiplied, among them the distinguished works of analysts such as Colin S. Gray (*The Geopolitis of Nuclear Era*, 1976), John G. Pappageorge (*Maintaining the Geostrategic Advantage*, 1977), Zbigniew Brzezinski (*Game Plan. Geostrategic Framework for the Conduct of the US-Soviet Contest*, 1986), Hervé Couteau-Bégarie (with three works having in the title the *Géostratégie* term, dedicated to South Atlantic, 1985, Pacific, 1987, and Indian 1993 Oceans), André Vigarié (*Géostratégie des océans*, 1990, *La Mer et la géostratégie des nations*, 1995), Amiral René Besnault (*Géostratégie de l'Arctique*, 1992) etc.

1. Confusions regarding the *geostrategy* concept

It might be noted that some analysts confuse the *geostrategy* concept with *Peace and conflict studies* (gr. polemos = war, logos = science), a branch of political science covering scientific study of wars, establishing its typology as a sociological phenomenon, its causes, effects, objectives and functions with the main purpose of removing them from our society. The term was introduced by french sociologist Gaston Bouthoul (1896-1980) in 1945, inspired by his french counterpart Rudolf Steinmetz, founder of a specialized institute in this area. Bouthoul will then write a paper (*Les guerres*, 1951), which will turn into a treaty (*Traité de polémologie. Sociologie des guerres*, first edition in 1970).

There are also other confusions that are made: some consider that *Geostrategy* is but another name for *Military Geography,* and others that is a branch of *Geopolitics*, that is studying in particular, security related issues.

There are analysts who simply consider it as a similar notion with *Geopolitics*. It should also be recognized that the relationship *Geostrategy-Geopolitics* is a very difficult one,

[3] Nicholas Spykman (1994), *The Geography of the Peace*, Harcourt Brace, New York, p. 6.
[4] George B. Cressey (1944), *Asia's Lands and Peoples. A Geography of One Third of the Earth and Two-Thirds of its People*, McGraw-Hill, II, New York, p. 32.

with a very permeable and hard to find border, many writers/analysts are simultaneously drawn to both areas, as noted, among others, the Moldovan analyst Oleg Serebrian. Is enough to just think of the American Alfred Thayer Mahan (1840-1914), author of *Sea Power theory* and British Halford J. Mackinder (1861-1947), creator of the opposite concept or theory, *Land Power* best known as the *Heartland theory* ("World Heart ")[5]. But there are many others, including Julian Corbett (1854-1922), also British, Virgilio Spiga (1907-1976), italian, both with significant contributions in the field of naval strategy.

Many authors from this field, among which the famous british historian Arnold Toynbee (1889-1975), explain the strategy evolution only, or almost exclusively, through the evolution of combat: phalanx – Legion (Romans) – Turcoman's bow – gunpowder – rapid firing gun – machine gun – railways – chariot and motorization – plane – atomic weapons etc., all scored major changes in the field. But, as general André Beaufre remarked, over 50 years ago, "it is true, improved technology is an essential factor of power. (...) But this progress/improvement can prove useless if it is used by a bad strategy. (...) Let us remember our recent experiences in Algeria [refers to French – our note], for example: did these new, modern weapons help us to achieve our purpose? In fact there are no such things like optimal tactics, any tactic has worth only in relation to the opponent. We have seen, for example, that the plane and chariot are put into difficulty by guerilla attacks and that the nuclear weapon would not allow the United States to gain an advantage in Korea, but only a compromise truce. This means that there is something that needs to dominate the tactics: *the choice of tactics* (emphasis added). *And the choice of tactics is the strategy*. That strategy is the one that will decide the form of conflict – offensive or defensive, insidious or violent, direct or indirect –, if you choose to fight in the political or military, whether to use or not use atomic weapons etc"[6].

In this context it should be noted that in the period after the Second World War, strategic studies have prevailed, especially thanks to the East-West confrontation, pure military studies, that eclipsed the geostrategy ones, although many elements were related to geostrategy. Of the former, some due to reputable geopoliticians, we remember some french analysts (Amiral Raoul Castex, *Théories stratégiques*, 1929-1939; André Beaufre, *Stratégie de l'action* 1966, *Stratégie pour domain. Les problèmes militaires de la guerre moderne* 1972, Jean-Paul Charnay, *Essai général de stratégie* 1973, *Métastratégie. Systèmes, formes et principes de la guerre féodale à la dissuasion nucléaire*, 1990, *La stratégie*, 1995; Hervé Couteau-Bégarie, *Traité de Stratégie*, 1999; Philippe Moreau-Defarges, *Problèmes stratégiques contemporaines,* 1992; Lucien Poirier, *Stratégie théorique*, three volumes, the first in 1982 *Essais de stratégie théorique*), american analysts (Colin S. Gray, *Strategic Studies and Public Policy*, 1982 *War, Peace and Victory: Strategy and Statecraft for the Next Century,* 1990, *Explorations in Strategy*, 1998; Peter Paret, editor, *Makers of Modern Strategy*, 1985; John Baylis and Ken Booth, *Contemporary Strategy – I. Theories and Concepts*, 1987, Kenneth N. Brown, *Strategic. The Logistic – Strategy Link*, 1987; John M. Collins, *Grand Strategy. Principles and Practices*, 1973, *Military Strategy. Principles and Historical Perspectives*, 2002; Bernard Brodie, *Strategy as a Science*, 1949, Edward N. Luttwak, *Strategy and History*, 1985; Paul Kennedy, editor, *Grand Strategies in War and Peace*, 1991) british analysts (Ken Booth, *Strategy and Ethnocentrism*, 1979, N.A.M. Rodger, *The Command of the Ocean. A Naval History of Britain* 1649-1815, three volumes, 2004; John Baylis and John Garnett, editors, *Makers of Nuclear Strategy*, 1991) german analysts

[5] For details see also: Aymeric Chauprade, François Thual (2004), *Dicţionar de geopolitică: state, concepte, autori*, Editura Corint, Bucharest, pp. 506-510; Silviu Neguţ (2008), *Geopolitica. Universul puterii*, Editura Meteor Press, Bucharest, pp. 32-38 etc.

[6] André Beaufre (1998), *Introduction à la stratégie*, Editura Hachette, Paris, pp. 69-70 (first edition was published in 1963, at Armand Colin Publisher house).

(Albert A. Stahel, *Klassiker der Strategie*. *Eine Bewertung*, 1996; Wilhelm Schaubourg-Lippe, *Schriften und Briefe. II Militärische Schriften*, 1977; plus dozens of books – not to mention articles –, dedicated to the great Prussian strategist Carl von Clausewitz), italian analysts (Carlo Jean, *Guerra, strategia e sicurezza*, 1997; Paulo Supino, *Strategia globale*, 1965), spanish analysts (Miguel Alonso Baqueria, *En quié consiste la estrategia?*, 2000; Fernando de Bordejé y Morenci, *España, poder maritimo y estrategia naval*, 1982), portuguese analysts (Virgilio de Carvalho, *Estratégia global e subsidios para una grande estratégia nacional*, 1986; Abel Cabral Couto *Elementos de estratégia*: *Apontamentos para um corso*, two volumes, 1988-1989), brazilian analysts (João Carlos Gonçalves Caminha, *Delineamentos de estratégia*, 1982).

2. Military Geography – precursor of Geostrategy

We can not imagine any state expansion in history and even less, the creation of great empires, all made by force, without knowledge of the natural environment and, especially, of how its elements could influence the military actions in question. All military commanders took account of it, from the ancients (Sun Zi, Cyrus the Great, Alexander the Great, Hannibal, Caesar, Trajan, etc) to the Middle Ages ones (Genghis Khan, Solyman the Magnificent, Peter the Great, Stephen the Great, etc) and to the modern times one (Napoleon Bonaparte and all the myriad of European, American and Asian generals that marked the last two centuries).

For a long time it was nameless, a while it was called *Military geography* defined briefly as *the science that studies the impact of geographical factors, particularly the landscape, water and climate, over the military actions*.

So, the Chinese general Sun Zi/Sun-tzu (VI-V B.C.), author of the first treaty of military strategy known until today (*Military Art*) stated, two and a half millennia ago: "Who does not known the forests and mountains configuration, gorges and swamps, can not make the military to move forward." It is also well-known that, more than a thousand years ago, Emperor Constantine VI Porphyrogenitus, when was preparing a campaign, started by learning about the operations scene (distance, resources, state roads and defence capabilities), as shown in his work *De administrando imperio*.

As well notifies the french analyst Hervé Couteau-Bégarie, the theoretical link between *geography* and *war* is clearly stated only in the 18th century in France (Abbot Lenglet-Dufresnoy, *Méthode pour étudier la géographie*, 1716 and *Introduction à la Géographie moderne* in " Encyclopédie méthodique. Géographie Moderne" 1^{ere} tom, 1782, better known as "Panckoucke Encyclopedia" after the name of the publishing house that published it). By the next century it was introduced not only in France but also in Germany, Austria, Spain, Italy, Russia and other countries, forming real schools on the subject. It is particularly significant the indication made in the mentioned encyclopedia: "A little trained general is shy; he will go in operations tapping, will swerve from his purpose, will consult other opinions, will hesitate... A trained military, a geography scientist general will know beforehand the advantages and disadvantages that may result from one or another position; he has already prepared the triumph on the map, even before seeing the enemy, he defeated".

Several schools of military geography were individualized in the second half of the 19th century, such as: French, German, Spanish, Italian, Austrian and Swiss, Russian, Anglo-Saxon and even a Romanian one.

Conclusions

After studying the concepts of *military geography*, *geostrategy*, *geopolitics*, were revealed the following conclusions:

- all these concepts were founded in the second half of 19th century, between them existing strong terminological, sometimes even notional, confusions;
- *geostrategy* term (Giacomo Durando, 1846) precedes the *geopolitics* one (Rudolf Kjellén, 1899), and other such as *geotactics,* disappeared due to the overlap with the high development of *Military geography* concept, which is why *geostrategy* returned into attention more later (at almost 100 years away, by George B. Cressey, 1944);
- at first sight some believed that *Geostrategy* is nothing but another name for *Military geography*, and by others that it was just another branch of *Geopolitics* that studies particularly security related problems.

BIBLIOGRAPHY:

2. Beaufre, André (1998), *Introduction à la stratégie*, Editura Hachette, Paris.
3. Botti, Ferrnicio (1995), *Le concept de géostratégie et son application à la nation italienne dans les théories du géneral Durando*, in „Stratégique", 58, 1995-2.
4. Chauprade, Aymeric; Thual, François (2004), *Dicţionar de geopolitică: state, concepte, autori*, Editura Corint, Bucharest.
5. Coutau-Bégarie, Hervé (2008), *Traité de Stratégie*, 6eme edition, Editions Economica, Paris.
6. Cressey, George B. (1944), *Asia's Lands and Peoples. A Geography of One Third of the Earth and Two-Thirds of its People*, McGraw-Hill, II, New York.
7. Neguţ, Silviu (2008), *Geopolitica. Universul puterii*, Editura Meteor Press, Bucharest.
8. Spykman, Nicholas (1994), *The Geography of the Peace*, Harcourt Brace, New York.

RUSSIAN MILITARIZATION OF THE ARCTIC

Cristina Simona BONDAR
PhD student, "MIHAI VITEAZUL" National Intelligence Academy
e-mail: cristinabondar@gmail.com

Abstract: *Increasing struggle for influence and energy pushed Russian Federation into a new arms race in the Arctic. For this purpose, Moscow is modifying the legislative framework, the new provisions stating that the Arctic Commandment will be created, the impressive military capabilities built during the Soviet era will be restored, new military bases will be opened and modern equipment will be delivered for them.*

While developing the military capabilities, Kremlin is conducting large Armed Forces applications, with a demonstrative role in international relations.

Keywords*: militarization, Russian Federation, Arctic Region*

Introduction

After the fall of the Iron Curtain, Arctic territory of silent confrontation between American and Russian submarines during the Cold War went into obscurity. This shadow started to rise with increasing energy needs of the world countries. The findings in this area indicate that there are approximately 13% of untapped oil reserves in the world and 30% of gas.

Due to the growing divergence between NATO and the Russian Federation, the tensions in the region will see an escalation caused by the proximity of the two actors.

Russia's Arctic policy is based on several strategic documents, among which there are:

- Fundamentals of State Policy of the Russian Federation in the Arctic by 2020, adopted in 2008;
- Military Doctrine of the Russian Federation in 2014;
- The National Security Strategy of the Russian Federation in 2020;
- Foreign Policy Concept of the Russian Federation published in 2013.

1. Interests of the Russian Federation in the Arctic

Lately was been observed a revival of interest from Moscow to the region, emphasizing the importance of the area to ensure security and economic objectives of the Russian Federation. In this regard, the Kremlin actions in the Arctic are covering several elements. The main component is the economic development of Russian territories. In addition, the state sees the region as a platform to promote Russia as a major world power.

According to estimates, by the middle of the 21st century, the ice cap will melt completely during the summer, which will allow the developing of new transport routes, safer and cheaper compared to those currently in transit through the Horn of Africa, the straits or the Suez Canal Malacca.

Along with economic interests, a very important element of Russian policy in the Arctic is the military perspective, the supremacy in Russia's far north giving the opportunity

to the state to have access to the ocean for its submarines with nuclear deterrent role in politics[1].

To achieve these goals, the authorities' mode of action includes territorial claims.

2. Actions mode of Moscow in the Arctic

Moscow treats any foreign interest towards this area, whether it is an economic, commercial and environmental like hostile intent, which led to a rhetoric and actions designed to intimidate the stakeholders of the region.

The Kremlin has sent numerous messages, both declarative and symbolic, to support territorial claims in the Arctic, many of them by trying imposing, sometimes in a quite aggressive way, of the sovereignty over territories. To this end, one of the main assertions is the idea that the Lomonosov and Mendeleev ridges are part of Russia's continental shelf, which would give the right under the Convention on the Rights of the Sea - UNCLOS, to claim 200 sea miles from land and exploit resources at a distance of 350 nautical miles. Russian Federation claims that the two forms of relief are not dorsals, but extensions of its continental shelf. On the other hand, and Denmark (through its sovereignty over Greenland) and Canada promotes the theory that Lomonosov is a part of their continental platforms. Granting territorial rights for any of these countries would considerably increase the area in which countries would be entitled to open mine or energy.

1) North Pole
2) Lomonosov Bridge
3) 200 marine miles, the exclusive economic area limit
4) land claimed by Russian Federation

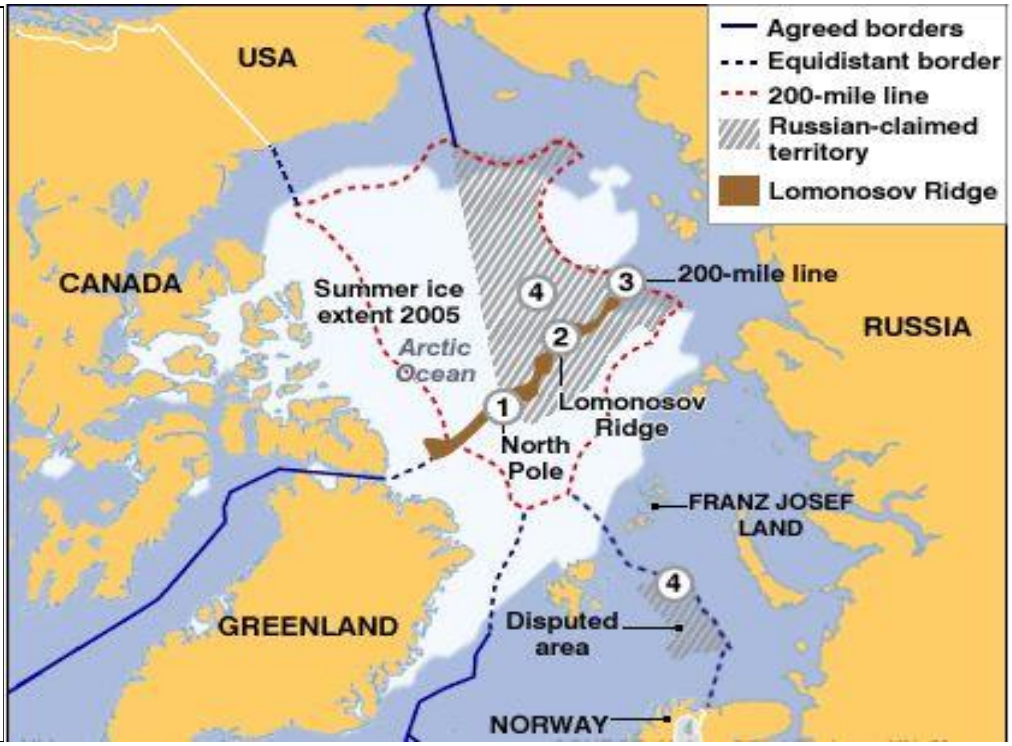


Figure no. 1, Land claimed by Russian Federation in the Arctica
Source: „BBC"

[1] SMITH Mark, A.; KEIR; Giles, *Russia and the Arctic: The "Last Dash North"*, Defence Academy of the United Kingdom, 2007, available at http://www.academia.edu/929852/Russia_and_the_Arctic_the_Last_Dash_North_, consulted at 01 March 2015

Although Moscow has submitted a request to the UN for recognition of the Lomonosov Ridge in 2001, a solution has not been adopted so far. According to statements made by Russian officials, this request will be renewed in 2015[2].

To strengthen these claims, Moscow has launched exploratory missions that were aimed at collecting samples from the ocean floor and bathymetric data. In addition, in 2007, two mini submarines, placed a titanium flag on the seabed near the North Pole. The action has generated criticism of Russia, being compared by the Canadian Foreign Minister at the time, as a colonization like in the XVth century[3]. The expedition itself was a demonstration, the icebreaker that released the submarines transported a deputy of the State Duma, and the ship was the one which managed to reach North Pole through ice cap cutting[4].

Another hot spot of the region and is the maritime border between the US and the Russian Federation, the treaty signed in 1990 being perceived by the Russian as unfair and negotiated on a time when the Soviet Union was about to collapse. Because of that, the document had not been ratified by the Russian parliament[5].

Another element on which the two countries failed to reach an agreement is the status of the Northern Route. While Washington is campaigning for the right of free navigation, Moscow claims that the route passes through its territorial waters and therefore it is necessary that ships transiting the area must request permission, and pay for the delivery of the Russian ice breakers[6].

3. The military component - central element of Russian policy in the Arctic

Foundations of State Policy of the Russian Federation in the Arctic by 2020 stipulates that o potential change the balance of power in the future, could determine Russia to defend the interests of the state by using military force. Since the Russian Federation is the state with the longest border to the Arctic, more than 6,000 kilometers, Moscow acts to secure its several ways.

Thus:

- Has reorganized the management structure of the operations in the North, creating the Joint Strategic Command;
- The Soviet-era military bases had been reopened and is planning to build new military facilities in the region;
- It is in a modernization process of military capabilities in the region;
- Plans to increase the number of soldiers posted in the Arctic.

Joint Strategic Command became operational on 1 December 2014. It is based on the Northern Fleet, which were transferred units, ships and troops of the Western, Central and South Military Districts of Russia. It will include two motorized infantry brigades, which are

---

[2] Declarație a ministrului resurselor naturale, Serghey Donskoy, după o întrevedere cu președintele Vladimir Putin în aprilie 2015; disponibilă la http://barentsobserver.com/en/arctic/2014/04/putin-readies-arctic-territorial-claims-07-04

[3] *Russia plants flag under N Pole*; available at http://news.bbc.co.uk/2/hi/europe/6927395.stm; 2 august 2007, consulted at 20.02.2015

[4]PADRTOVA, Barbora, *Russian Approach Towards the Arctic Region*, 2012, available at http://cenaa.org/analysis/russian-approach-towards-the-arctic-region/, consulted at 15 february 2015

[5] KACZYNSKI, Vlad M., *US-Russian Bering Sea Marine Border Dispute: Conflict over Strategic Assets, Fisheries and Energy Resources*, Russian Analytical Digest, may 2007, available at http://www.css.ethz.ch/publications/pdfs/RAD-20-2-5.pdf , consulted at 21 march 2015

6 ROSEN, Mark E.; ASFURA-HEIM Patricio, *Addresing the gaps in Arctic Governance*, octomber 2013, available at http://www.hoover.org/research/addressing-gaps-arctic-governance, consulted on 10 february 2015

designed to support and escort vessels using the Northern Route[7]. The presence of special forces has increased by 30% through revitalization of the 61st Infantry Regiment Independent Naval, who will stand alongside The Independent Infantry Brigade 200, in Sputnik Base, a restored soviet site, inside the Polar Circle at a distance of 16 kilometers from the border with Norway, and 65 kilometers from the Finland.

According to the media, the Joint Strategic Command will operate and Panţir type-1 rocket and artillery systems, helicopters modified for cold climate - Mi-8 Hip and MiG - 31 Foxhound airplanes[8].

In addition, by the end of 2015 was announced the completion of modernization and reopening military bases built in the Soviet period and the opening of new facilities. Is retaining attention that a new military base is been constructed in an area classified by the Russian authorities as a natural reserve, Wrangel Island[9].

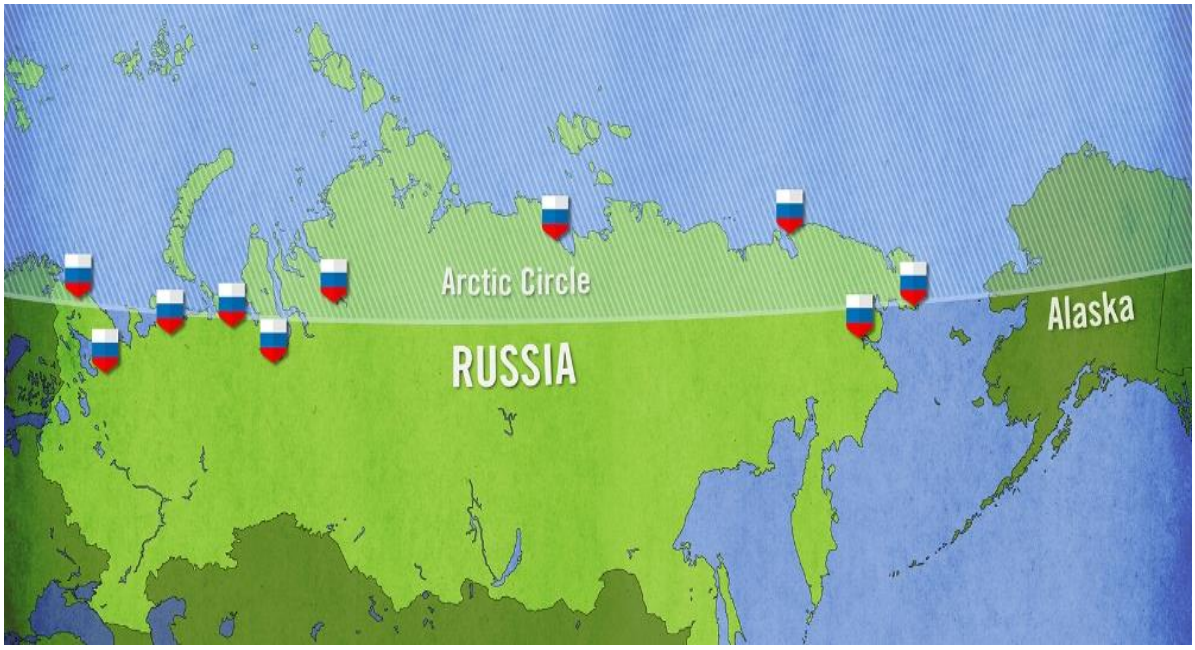


Figure 2, Russian military bases in the Arctic
Source: http://www.globalsecurity.org/military/world/russia/vo-northern.htm

In addition, there will be reactivated and built radar stations, their total number will reach six[10]. To increase the ability to monitor, Russia intends sending in the Arctic drones Orlan-10, with an autonomy of 16 hours and an operational area of 600 km[11].

---

[7]*Russia to Form Arctic Military Command by 2017*; 1 October 2014, available at http://www.themoscowtimes.com/business/article/russia-to-form-arctic-military-command-by-2017/508199.html, consulted at 15 March 2015.

[8]JENNINGS, Gareth, *Russia to build more Arctic airfields*, 12 January 2015, available at http://www.janes.com/article/47831/russia-to-build-more-arctic-airfields, consulted on 15 March 2015

[9]*Russia to Form Arctic Military Command by 2017*; 1 October 2014, available at http://www.themoscowtimes.com/business/article/russia-to-form-arctic-military-command-by2017/508199.html, consulted at 15 March 2015

[10]*Joint Strategic Command*, available at http://www.globalsecurity.org/military/world/russia/vo-northern.htm, consulted on 14 March 2015.

The Arctic, unlike the Black Sea or Baltic Sea, offers to Russia the possibility of direct access to the world's oceans, being the reason for sending in the area the most powerful of its fleet, the Northern Fleet. The structure includes nuclear submarines, strategic bombers and intercontinental missiles.

With the reduction of Russian conventional military capabilities, the importance of Moscow nuclear deterrence policy has increased, Russian Federation trying to recapture the title of naval power. In this regard, a high priority was given to modernizing the nuclear arsenal, including the construction of a new multirole submarine from Yassen class and placing orders for other ships of this type, such as purchase intentions more Borei class submarines capable carry ballistic missiles[12].

Along with purely military capabilities, the Russian Federation is the only state that has a fleet of nuclear-powered icebreakers, the last one entered service being the most powerful - "50 Years of Victory". These vessels have a decisive role in the transit of any civil or military surface vessels, facilitating both compact pack ice crossing and the traveling through dangerous waters due to detachment of glaciers.

4. Difficulties in implementing the Russian strategy for the Arctic

Although there has been a rise in military activity and were implemented concrete steps to modernize Russian forces in the region, these developments took place amid the existence of a weaken Army. The pace of innovation has been slow, despite some radical reforms.

Even there were some bellicose statements, the experts pointed out that the capabilities available to the Russian Federation is not a threat so great comparing to the delarations. In this respect, Alexandre Golts argue that Moscow's aggressive speech extends over a long period of time but far from all its grand plans, had been deployed only two brigades consisting of dozens of people. Even though their number would be higher, it would be impossible to provide effective security to the Arctic coast from Murmansk to Vladivostok. However, the soldiers did not even have a purely military role being used to build a new military base. At this point, adding the logistical elements, the process of stocking for bases from the Arctic Circle is difficult, especially with the fuel needed for patrol missions.

Experts argued that impressive military exercises have shown a lack of preparedness of forces in the Arctic. The scenario used in the last one was a Cold War tactic, involving the identification and destruction of submarines and aircraft carriers groups. For those action, had been used a group of soldiers from central Russia. On the other hand, the Arctic brigades have served to neutralize the subversive groups that appeared exactly in territory controlled by them[13].

Their deployment locations, far from the territories under dispute, induce the idea that their maneuver was a public demonstration, and it wasn't a simulation of a real situation in which they might be involved in warfare.

---

[11] *Russia plans Orlan-10 UAV Arctic deployment*, 7 January 2015, available at http://www.janes.com/article/47732/russia-plans-orlan-10-uav-arctic-deployment;%20Russia%20plans%20Orlan-10%20UAV%20Arctic%20deployment;%207%20ianuarie%202015, consulted on 16 March 2015.

[12] STAALESEN Atle, *New attack submarine ready before year's end*, Barents Observer, 20 August 2012, http://www.barentsobserver.com/en/security/new-attack-submarine-ready-years-end-20-08, consulted on 10 March 2015.

[13] GOLTS, Alexander, *Why Russia's War Games Should Scare Nobody*, 23 March 2015, available at http://www.themoscowtimes.com/opinion/article/russia-s-war-games-should-scare-nobody/517898.html, consulted on 28 March 2015.

Another element that will significantly affect Moscow capabilities in the area and close is the decommissioning of nuclear icebreakers available in the present. In the absence of clear plans for the construction of new vessels, the prediction made in 2012 by the Atomflot Director, Viacheslav Ruksha, who said that during 2016-2017, Russia will suffer a collapse in is area, it is likely to became a truth[14].

Conclusions

Despite the extremely ambitious plans of Russian authorities for the Arctic, the probability of their materialization is quite low. This is mainly due to a lack of financial resources directed to this objective. Along with the reduction in income as a result of Western imposing sanctions to Russia after the annexation of Crimea and for the support given to the rebels in Donetsk and Luhansk, those measures reduced the access to military and civilian technologies that can be used in the area.

This led, in part, to a reduced equipment modernization and construction of new ones, Ukraine being one of the main suppliers of components used in the industry. On the other hand, the sanctions have led to a reluctance of Western companies to invest in the exploitation of hydrocarbon deposits, which became an impediment to the economic development of the region. At this point, decrease in oil prices also contributed to weakening the Russians plans, this aspect being another blow to already hurt economy.

In addition, the northern route is not currently viable for use by commercial vessels, to the increased costs for infrastructure being added some exorbitant insurance companies taxes.

However, although the pace of implementation of reforms will continue to be low, the Kremlin will not give up ambitions to impose Russia as the most important actor in the Arctic, both economically and militarily.

BIBLIOGRAPHY:

1. FAITH, Ryan, *Russia's Massive Military Exercise in the Arctic Is Utterly Baffling*, 21 March 2015, available at https://news.vice.com/article/russias-massive-military-exercise-in-the-arctic-is-utterly-baffling, consulted on 28 March 2015.
2. GOLTS, Alexander, *Why Russia's War Games Should Scare Nobody*, 23 March 2015, available at http://www.themoscowtimes.com/opinion/article/russia-s-war-games-should-scare-nobody/517898.html, consulted on 28 March 2015.
3. JENNINGS, Gareth, *Russia to build more Arctic airfields*, 12 January 2015, available at http://www.janes.com/article/47831/russia-to-build-more-arctic-airfields, consulted on 15 March 2015.
4. Joint Strategic Command, available at http://www.globalsecurity.org/military/world/russia/vo-northern.htm, consulted on 14 March 2015.
5. KACZYNSKI, Vlad M., *US-Russian Bering Sea Marine Border Dispute: Conflict over Strategic Assets, Fisheries and Energy Resources*, Russian Analytical Digest, May 2007, available at http://www.css.ethz.ch/publications/pdfs/RAD-20-2-5.pdf , consulted at 21 March 2015.

[14] FAITH, Ryan, *Russia's Massive Military Exercise in the Arctic Is Utterly Baffling*, 21 March 2015, available at https://news.vice.com/article/russias-massive-military-exercise-in-the-arctic-is-utterly-baffling, consulted on 28 March 2015.

6. PADRTOVA, Barbora, *Russian Approach Towards the Arctic Region*, 2012, available at http://cenaa.org/analysis/russian-approach-towards-the-arctic-region/, consulted at 15 February 2015.
7. ROSEN, Mark E.; ASFURA-HEIM Patricio, *Addresing the gaps in Arctic Governance*, October 2013, available at http://www.hoover.org/research/addressing-gaps-arctic-governance, consulted on 10 February 2015.
8. *Russia's Arctic Strategy*, available at https://archive.org/stream/563663-russias-arctic-strategy/563663-russias-arctic-strategy_djvu.txt, consulted on 20 February 2015 .
9. *Russia plants flag under N Pole*; available at http://news.bbc.co.uk/2/hi/ europe/6927395.stm; 2 August 2007, consulted at 20 February 2015.
10. *Russia plans Orlan-10 UAV Arctic deployment*, 7 January 2015, available at http://www.janes.com/article/47732/russia-plans-orlan-10-uav-arctic-deployment;%20Russia%20plans%20Orlan10%20UAV%20Arctic%20deployment;%207%20ianuarie%202015, consulted on 16 March 2015.
11. *Russia to Form Arctic Military Command by 2017*; 1 October 2014, available at http://www.themoscowtimes.com/business/article/russia-to-form-arctic-military-command-by-2017/508199.html, consulted at 15 March 2015.
12. SMITH Mark, A.; KEIR; Giles, Russia and the Arctic: The "Last Dash North", Defence Academy of the United Kingdom, 2007, available at http://www.academia.edu/929852/ Russia_and_the_Arctic_the_Last_Dash_North_, consulted at 01 March 2015.
13. STAALESEN Atle, New attack submarine ready before year's end, Barents Observer, 20 August 2012, http://www.barentsobserver.com/en/security/new-attack-submarine-ready-years-end-20-08, consulted on 10 March 2015.
14. STAALESEN, Atle, Putin readies Arctic territorial claims, 07 April 2012, available at http://barentsobserver.com/en/arctic/2014/04/putin-readies-arctic-territorial-claims-07-04, consulted at 05 March 2015.
15. ZYSK, Katarzyna, *Russia's Arctic Strategy, Ambitions and Constraints*, Norwegian Institute for Defence Studies, 2010, available at http://www.ndu.edu/press/ lib/images/jfq-57/zysk.pdf, consulted on 20 February 2015.

RESOURCE ALLOCATION AND CAPABILITIES GENERATION IN SECURITY STUDIES

Mihai ZODIAN, PhD
Junior researcher at the Center for Strategy, Defence and Security Studies at the Naţional Defence University „Carol I", Bucharest, Romania.
zodian@gmail.com

Abstract: *Security studies developed after Cold War's end, in an attempt to push the intellectual and public agenda beyond the traditional themes related to the use of military force. This paralleled a wider societal interest in enjoying the benefits peace and welfare, based on an optimistic view of international affairs and of politics, in particular, which was tested each time when crisis and conflicts erupted or gained public attention. This paper traces the evolution of security studies and their relationship with military power, arguing that this theme deserves more scrutiny, because of theoretical and political significance.*

Keywords: *security, capabilities, military power, realism, constructivism*

This paper aims to investigate the continuities and changes which characterize the security studies discipline after Cold War's ending, from the perspective of resource allocation and capabilities generation. The subject grew in importance after the economic crisis starting in 2007-2008 and became fundamental in the recent context of the conflict in Ukraine. The academic trends may offer a representation of social reality, but also they can say a lot about current mentalities or even influence policy, under favorable circumstances.

More precisely, one can noticed diverging trends inside of transatlantic community regarding what is important as far as the security domain is concerned, the meaning of this term and the policies which various actors pursue[1]. This pluralism of interpretations parallels different approaches shared by decision-makers after the Cold War regarding threat framing, allocation policies, the right balance between various societal sectors and the range of strategies. Key issues involved were the attitude towards the use of force, budgetary politics, economic development or the value of identity as stimulus for political behavior.

The relationship between research and practice is often discussed in academic circles, but its nature still remains ambiguous. The various approaches alternate between a reflective view, where the studies reproduce the reality of the security environment, and a more activist or critical view, where ideas are part of a social structure which they help into configuring[2]. This paper will not try to solve this complicated issues, but will focus on the describing the main trend of security studies discipline, using the resource allocation for security studies as lens.

Beyond paradigms

In the often used kuhnian terms, the social sciences, including the strategic and security studies are strongly influenced by paradigmatic changes, more precisely, by the ones regarding fundamental assumptions and mental structures on which research is based,

[1] Robert Kagan, *Dincolo de paradis şi putere*, Antet, Bucureşti, 2005; Felix Ciută, „Mythologies of European Security", conference at NSPSA, Bucharest, Romania, july 2014.

[2] Ole Waever, "Figures of International Thought: Introducing persons instead of paradigms", în Iver B. Neumann, Ole Waever, *The Future of International Relations*, *Masters in the Making*, Routledge, 1997, pp. 2-30.

defining how we see the problems, what concepts are we using and what methods we prefer[3]. This concept allows to link social traits and intellectual trends in a dynamic way, while avoiding the pitfalls of both materialistic and idealistic approaches. The weakness consists in the implicit relativism of social and historical contextualization, at least for the natural sciences, while as its author intended, the term paradigm is almost impossible to be used with rigor in the social sciences, including in the security and strategic studies[4].

But not for lack of trying. Guzzini argued that realism played the role of paradigm, of a mental structure which attempts to define an academic domain, especially in the United States[5]. After the Cold War, especially in the EU, an attempt to develop an alternative paradigm, which put more value on civilian aspects of security[6]. This tendencies lead to a theoretical pluralism, even if the security domain seemed similar. Thus, in our domain, the main changes after the end of Cold War subordinated the traditional concerns regarding the use of force to themes like new threats, identity issues, debates about state's future as an international actor, the role played by the distribution of capabilities, and the tendency of engulfing the strategic studies into a wider new security studies research domain[7].

The problem here regards the adequacy of paradigm as a tool for understanding the continuities and changes in the social sciences in general and in security studies in particular. Besides the well known skepticism expressed by Kuhn himself, this particular notion underestimate the normative and political laden nature of these domains. No common view can last for long, because opinions and interests diverge, while methods are ambiguos.

An alternative is offered by the truth regimes concept used by Michel Foucault, one of the most influential postmodernist philosophers, and extended to security studies by authors like Bradley Klein[8]. This concept starts from criticizing the assumption of an essential unity defining security or strategic studies, being inspired by a more pluralistic and potential polemic view of knowledge production, which is closer to the way in which social sciences look on the long term. Power and knowledge are linked by behaviors and practices, which are correlated and receive meaning from these intellectual schemes, which are both inspired by and creators of social reality[9]. Thus, the point is not exactly, in this view, about explanatory power, but by the reasons which are giving these formulas credibility, even though they are ambiguous and potentially contradictory[10].

We shall see that the ontological status of security and strategic studies is open to changes, depending on the points of view shared by various researchers. Even in this paper,

---

[3] Thomas Kuhn, *Structura revoluţiilor ştiinţifice*, Humanitas, 2008.

[4] *Ibidem*, p. 58; Martin Curd, J. A. Cover, *Philosophy of Science. The Central* Issues, W.W. Norton and Company, 1998, pp. 210-251.

[5] Stephano Guzzini, *Realism şi relaţii internaţionale*, Institutul European, Iaşi, 2000. A good discussion on security can be found in Radu-Sebastian Ungureanu, „Extending the concept of security" and „The concept of security" in Andrei Miroiu, Radu-Sebastian Ungureanu (coord.), *A Handbook of International Relations*, (Romanian version "Extinderea conceptului de securitate", in Andrei Miroiu, Radu-Sebastian Ungureanu (coord.), *Manual de relatii internationale*, Polirom, Iasi, 2008.

[6] For the specifics of european approaches to security, see Felix Ciută, „Mythologies of European Security", conference at NSPSA, Bucharest, Romania, july 2014.

[7] Exemplary for this approach is Barry Buzan`s work, *People, states and fear* (Romanian edition *Popoarele, statele şi teama*, Cartier, Chişinău, 2000). See also Radu-Sebastian Ungureanu, *op. cit.,* pp. 186, 187-198.

[8] Michel Foucault, *Naşterea biopoliticii*, Idea, Cluj, 2007, p. 28; Bradley Klein, *Strategic Studies and World Order*, Cambridge University Press, 1994, pp. 3-12: Alan Collins, *Contemporary security* studies, pp. 78-81. O abordare apropiată, ce a securitizării, induce o diferenţă exagerată între securitate şi putere. Vezi Buzan, Barry, Waever, Ole, *Securitatea. Un nou cadru de analiză*, CA Publishing, Cluj 2001.

[9] *Ibidem*, p. 13. Columbia Peoples, Nick Vaughan-Williams, *Critical Security Studies: An Introduction,* Routledge, 2015, pp. 79-83.

[10] Ibidem, pp. 13, 29.

we discussed mostly authors from the „anglo-saxon" space, which are configuring the debates, even though the intellectual developments are more pluralistic. For example, in Romania, one can find, besides the two aforementioned disciplines, overlaps with International Relations, political sciences, sociology, history and especially with geopolitics, even if the last approach is riddled with logical flaws, the same way in which, in "The West", realist practices can mingle with liberal ideas[11].

Often it seems that what matters more than the content are the ways in which these approaches unify behavior and give them meaning. The consequence is that the difference between traditionalists and reformers, or the one between American and European practices is not reducible to the contrast of power and weakness, as Kagan thought[12]. More likely, it is about different modalities of thinking and using power, one inspired by realism and liberalism, in which the military sphere is distinct, and another, more globalizing, which projects a reform project unto whole societies, but in a decentralized way[13].

The consequence of using the truth regimes idea is that we should expect close relationship between power and knowledge, even if we are speaking of academics or habits. Since they can inspire ambiguous and potential conflictive relationships, social sciences are expected to look more polemical and controversial, with attempts for unification doomed to failure. Meanwhile, we should be wary of exaggerating the relationships between these two aspects, since differences remain.

The following parts of this paper will review some influential synthesis works published after the Cold War in the security studies domain[14]. Most of them are collective in nature and aim towards capturing the entire domain of security and strategic studies. The issues of military force and ideas/identity/values/norms will inform the structure of the analysis.

From Military Power to Identity and Back

In this paper, four works are considered, which can be seen as a landmarks for the trends previously discussed. The changes and the growing pluralism can be seen in an incremental fashion, in parallel with sometimes pretty intense theoretical struggles. The main issues involved are the use of military force, the role of state, the explicative value of power versus identity, new views on security and the rise of various intellectual programs which put realism and rationalism under question such as constructivism and critical theory.

Resource allocation represents a fundamental aspect of politics, one of the reasons why the concept of truth regimes works here[15]. Generally speaking, one can expect that intellectual formulas favorable to military power to promote more spending, under the limits suggested by prudence. The critical ones should tend towards a diversification of distribution. But both are interested in power, way to use it and to think about it. Thus, even when is not directly approached, the resource allocation agenda is implicit in the discussion about capabilities and the role of the state.

In a collective volume published in 1997, Craig Snyder argued in favor of extending the meaning of security towards more issues than the ones related to the use of force[16]. The

---

[11] Sergiu Tămaş, *Geopolitica. O abordare prospectivă*, Noua Alternativă, Bucureşti, 1995; Hans Morgenthau, *Politica între naţiuni. Lupta pentru putere şi lupta pentru pace*, Polirom, Iaşi, 2007, pp. 195-196.

[12] Kagan, *op. cit.*; Ciută, *op. cit*.

[13] Foucault, *op. cit*, pp. 15-17. Rita Floyd, „When Foucault met security studies: A critique of the Paris school of security studies", 2006 BISA annual conference.

[14] Kuhn, *op. cit.*

[15] Gøsta Esping-Andersen, *The Three World of Welfare Capitalism*, Princeton University Press, 1990.

[16] Craig Snyder, "Introduction", in Craig Snyder (coord.), *Contemporary Security and Strategy*, MacMillan, Ebbw Vale, 1999, p. ix.

reasoning was centered on an interpretation of 1989-1991 events, which lead to the decline of realism, the former dominant International Relations theory, which privileged states and force as fundamental subjects, while aiming towards both a broader theoretical range and for different policy themes[17]. Strategic studies were interested, traditionally in the efficiency of force in realizing political goals, which meant research subject as nuclear deterrence and limited wars and were profoundly influenced by the American academic and political environment[18]. He argued that a similar approach was formed in the United Kingdom, called security studies, but with a difference, coming from critical studies, which lead to a search for theoretical alternatives to the bipolar competition, during which these domains developed.

Once the Cold War ended, military force receded as importance in international relations, with the rise of unipolarity, at least for the short term. This phenomena paralleled the growing importance of various cultural interpretations like constructivism, which put a premium on interest and identities structures, instead of capabilities and material factors, as sources of explanation[19]. Thus, the concept of security required broadening, for many authors, which meant at least studying internal determinants of policy or new threats for the author[20]. Even so, Snyder and other authors kept state's role as the main institution responsible of security issues and the traditional subject of strategic studies discipline[21].

The parallel tendencies of conceptual broadening and creating a new domain were reflected in the work authored by Barry Buzan, and Lene Hansen, *The Evolution of International Security Studies,* published in 2000[22]. Buzan was one of these changes main promoters, and a part of Copenhagen school, which played a major role towards the development of security studies once the Cold War ended. The new discipline tended, for the authors, to be defined around four issues: state's function on the international stage, the relationship between internal and external threats, extending the range of issues and the conflictual inherent to the concept of security[23]. Buzan and and Hansen correlated more intellectual approaches, though, including strategic studies, polemology, political sciences and international relations[24].

They argue that strategic studies started, after 1945, as a result of bipolarity and nuclear problematic, involving civilian researchers like Bernard Brodie or Thomas Schelling in debating the themes related to the use of military force[25]. The main intellectual result was deterrence theory, the idea that mutual assured destruction will result in maintaining some stability in international relations, because both superpowers, United States and Soviet Union had response forces invulnerable to first strike[26]. Thus, this research domain was strongly influenced by practical concerns and the American context of its origins, and replaced older approaches like geopolitics, but it had its own critics and controversies[27].

Similar to Snyder, Buzan and Hansen thought that the ending of Cold War changed in a fundamental way strategic studies. Even so, they didn't push for a linear approach, but they highlighted the cleavages and internal tensions of these research programs, especially between

---

[17] Craig Snyder, "Contemporary Security and Strategy", in Craig Snyder (coord.), *Contemporary Security and Strategy*, MacMillan, Ebbw Vale, 1999, pp. 2-3.
[18] *Ibidem*, p. 4.
[19] *Ibidem*, p.7.
[20] *Ibidem*, pp. 7-8.
[21] *Ibidem*, p. 2.
[22] Barry Buzan şi Lene Hansen, *The Evolution of International Security Studies*, Cambridge University Press, 2009.
[23] Buzan, Hansen, *op. cit*., pp. 10-13.
[24] *Ibidem*, pp. 14-15.
[25] *Ibidem*, p. 66.
[26] *Ibidem*, pp. 73-83.
[27] *Ibidem*, p. 1, pp. 101-104.

reformers, interested in broadening, and traditionalists, who wanted to keep the focus on the use of military power[28]. The first group pursues a rationalist/positivist epistemology, keep the focus on coercion, and is interested in issues like potential conflicts between Great Powers or the Revolution in Military Affairs[29].

The reformers promote a study agenda regarding non-military views on security, interdependence and the importance of identity on world politics[30]. As the authors recognize, this bycephalism is not new, but traces its origins in the famous work authored by Keohane and Nye, *Power and interdependence,* published in 1977[31]. Buzan and Hansen highlighted that the changes in strategic/security studies are not simply intellectual, but they are cause by a combination of factors including relationships between major actors, technological change, events, internal debates and institutional constraints[32]. In the end, they pointed out that the themes related to a broader view on security will remain in discipline's memory[33].

The intellectual success of reformers, at least in Western Europe, can be seen in the handbook coordinate by Paul Williams, *Security Studies[34]*. The themes unite classical issues like war and terrorism with reformer's favorite subjects such as human security, poverty, migration, transnational crime, with security dilemma, ethnic conflicts and alliances being in-between research items. But the interpretation is mostly on the promoter's side. Thus, for the editor, security is a concept whose meaning is influenced by political disputes, a typical idea for critical theories, but not only to them[35]. Considering that context is an important factor in the pragmatic interpretation of security, Williams argued that research approaches most break the links with International Relations theory, as a result of trends like the reduction of state's influence, the US intellectual influence and interdisciplinary[36].

Like Snyder, Buzan and Hansen, for Williams the main two trends in the security studies domain are the one interested in power, both as a source of explanations and as a tool for pursuing national interests, and the others which promotes emancipation as an answer, though with a utopian touch[37]. The coherence of referent objects, of the public and of the instruments used in assuring security were put under scrutiny[38]. This reflects the impacts of constructivism, critical theory and postmodernism, which put under question traditional distinctions in social studies.

Thus, for reformers, the process of broadening the sphere of security started from considering new approaches regarding the use of force, passed to a stage where the term's meaning and range were extended to include new object and sectors, but with the risk of covering the whole domain of politics. The studies on strategy and use of force were put on a relatively secondary spot, especially in Europe. State's role in defining international relations was put under question, identity replaced power as fundamental cause and a plurality of actors drew researchers attention.

Not all experts were convinced by these arguments, because they though that extending security's meaning was either an exaggeration, either a fashion typical to peaceful periods. They were more often found in the United States, though critical theories also

---

[28] *Ibidem*, p. 156.
[29] *Ibidem*, pp. 156-157, 165-170, 170-176.
[30] *Ibidem*, pp. 187-191.
[31] Robert Keohane, Joseph Nye Jr, *Power and interdependence* (romanian edition, Robert O. Keohane, Joseph Nye jr., *Putere şi interdependenţă*, Polirom, Iaşi, 2009).
[32] Buzan, Hansen, *op. cit*., pp. 41-65.
[33] *Ibidem*, p. 272.
[34] Paul D. Williams, *Security Studies: An Introduction*, Routledge, f.l., 2008.
[35] Paul D. Williams, "Security Studies", în *Security Studies: An Introduction*, Routledge, f.l., 2008, p. 1.
[36] *Ibidem*, pp. 4-5.
[37] *Ibidem*, p. 6.
[38] *Ibidem*, pp. 6-10.

developed across the ocean. Typical for the traditional approach is the volume *Strategy in the Contemporary World*, coordinated by John Baylis, James Wirtz, Colin S. Gray and Eliot Cohen, which is another handbook and reflects thus a consensus[39]. For the authors, there is a recurrent tendency of interest and neglect in strategic issues, which is determined by current events[40]. The reformists rise was, thus the result of hopes risen by the end of Cold War, and doesn't necessary point to a lasting progress[41].

On the contrary, for Baylis and Wirtz, the central notions rely on the traditional concept of strategy as a link between military means and goals influenced by politics, social and culture, while highlighting the similarity between this conception and realism, a pessimistic theory from the international relations domain, critical of notions like progress, and promoters of prudence and rationality as values[42]. It is important to add that the authors rejected reformist critiques regarding the closeness between experts and political decision centers[43]. Thus, for Baylis and Wirtz proposals aimed at limiting the attempts to integrate strategic studies in a wider security studies domain, by pointing out the role of force and the risks posed by conceptual ambiguity implied in the broadening of this concept[44]. In the end, they move towards the opposite of Snyder's framework; new problems, old approaches[45].

Thus, one can notice a growing divergence between various approaches regarding the traits of security. Rationalism and the use of military force are more accentuated on the other side of the Atlantic, while identify and civilian aspects are more important in Europe. These go in paralleled with different threat perception, strategic policies and decision-making procedures.

Conclusions

The purpose of this paper was to review the security studies literature, while pointing out the growing pluralism of this domain. Contrary to the concept of paradigm, we found out that no dominant view of the world emerged after the end of the Cold War. Thus, the utility of this concept in treating the social related academic disciplines is open to doubt, besides the many critiques which it received in the philosophy of science.

The linkages between power and knowledge becomes clearer now, on the background of diversity. Since no dominant view emerged, the results is kind of a conceptual chaos. Sometimes those disciplines seemed identical, otherwise different; sometimes they were seen autonomous, other times, integrated; sometimes the focus was on military force, other times a broader view is shared…

Snyder *et al* made a major step towards seeing old issues in new ways, including on issues like the explanatory power of concepts like the distribution of capabilities. This view is linked to the growing wave of critics which realism, especially the structuralist version had to adapt to. But the complex interaction between theory and facts pushed the strategic/security approaches further.

Buzan and Hansen offered a balanced view regarding the broadening of security process, by pointing out the divergence into two pathways. On one side, the reformers tried to offer a new view, defined by multiple sectors, multiple actors, a civilian approach and a

[39] John Baylis, James Wirtz, Colin S. Gray, Eliot Cohen (coord.), *Strategy in the Contemporary World*, Oxford University Press,Bath, 2007.
[40] John Baylis, James Wirtz, "Introduction", în John Baylis, James Wirtz, Colin S. Gray, Eliot Cohen (coord.), *Strategy in the Contemporary World*, Oxford University Press,Bath, 2007, p. 2.
[41] *Ibidem*, p. 3.
[42] *Ibidem*, pp. 4-9.
[43] *Ibidem*, pp 11-12.
[44] *Ibidem*, p. 13.
[45] *Ibidem*, p. 4.

special focus on identity, on the other side, the traditionalists were interested on research issues like the Revolution in the Military Affairs.

The volume coordinated by Paul Williams enshrined the reformer`s view on security affairs. The number of threats is increasing, while the political nature of these issues under consideration was approached from a critical perspective. This broadening of meaning and of content risked including everything under the cover of security, with a risks of confusion and resource stretching.

Last but not least Baylis *et al* tried to adapt the traditional perspectives, especially classic realism, to the security events seen once the Cold War ended. The strategic studies specific was pointed out, consisting in the many uses which military force can have in the new strategic context, from deterrence to conterproliferation. The broadening approach was at least sidelined.

Aknowledgement:

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. Baylis, John, Wirtz, James, "Introduction", în Baylis, John, Wirtz, James, Gray, Colin S., Cohen, Eliot (coord.), Strategy in the Contemporary World, Oxford University Press,Bath, 2007.
2. Baylis, John, Wirtz, James, Gray, Colin S., Cohen, Eliot (coord.), Strategy in the Contemporary World, Oxford University Press,Bath, 2007.
3. Buzan, Barry, Popoarele, statele şi teama, Cartier, Chişinău, 2000.
4. Buzan, Barry, Hansen, Lene, The Evolution of International Security Studies, Cambridge University Press, f.l., 2009.
5. Ciută, Felix, "Mythologies of European Security", prezentare în cadrul SNSPA, 10 iulie 2014.
6. Collins, Alan, *Contemporary security studies*, Oxford University Press, 2013
7. Curd, Martin, Cover, J. A., Philosophy of Science. The Central Issues, W.W. Norton and Company, 1998,
8. Esping-Andersen, Gøsta, *The Three World of Welfare Capitalism*, Princeton University Press, 1990.
9. Floyd, Rita, „When Foucault met security studies: A critique of the Paris school of security studies", 2006 BISA annual conference.
10. Foucault, Michel, Naşterea biopoliticii, Idea, Cluj, 2007
11. Keohane, Robert O., Nye jr., Joseph, Putere şi interdependenţă, Polirom, Iaşi, 2009.
12. Klein, Bradley, *Strategic Studies and World Order*, Cambridge University Press, 1994.
13. Kuhn, Thomas, Structura revoluţiilor ştiinţifice, Humanitas, 2008.
14. Kagan, Robert, Dincolo de paradis şi putere, Antet, Bucureşti, 2005;

15. Miroiu, Andrei, Ungureanu, Radu-Sebastian, (coord.), Manual de relaţii internaţionale, Polirom, Iaşi, 2006.
16. Morgenthau, Hans, Politica între naţiuni. Lupta pentru putere şi lupta pentru pace, Polirom, Iaşi, 2007
17. Peoples, Columbia, Vaughan-Williams, Nick, *Critical Security Studies: An Introduction,* Routledge, 2015.
18. Snyder, Craig, "Contemporary Security and Strategy", în Snyder, Craig, (coord.), Contemporary Security and Strategy, MacMillan, Ebbw Vale, 1999.
19. Snyder, Craig, "Introduction", în Snyder, Craig, (coord.), Contemporary Security and Strategy, MacMillan, Ebbw Vale, 1999.
20. Snyder, Craig, (coord.), Contemporary Security and Strategy, MacMillan, Ebbw Vale, 1999.
21. Tămaş, Sergiu, Geopolitica. O abordare prospectivă, Noua Alternativă, Bucureşti, 1995
22. Ungureanu, Radu-Sebastian, "Extinderea conceptului de securitate", în Miroiu, Andrei, Ungureanu, Radu-Sebastian, (coord.), Manual de relaţii internaţionale, Polirom, Iaşi, 2008
23. Ungureanu, Radu-Sebastian, "Conceptul de securitate", în Miroiu, Andrei, Ungureanu, Radu-Sebastian, (coord.), Manual de relaţii internaţionale, Polirom, Iaşi, 2008.
24. Waever, Ole, "Figures of International Thought: Introducing persons instead of paradigms", în Neumann, Iver B., Waever, Ole, The Future of International Relations, Masters in the Making, Routledge, 1997
25. Williams, Paul D.,, "Security Studies", în Paul D. Williams, Security Studies: An Introduction, Routledge, f.l., 2008.
26. Williams, Paul D.,, Security Studies: An Introduction, Routledge, f.l., 2008.

CIVIL-MILITARY INTERACTION AND CIVIL-MILITARY COOPERATION – TWO ESSENTIAL FEATURES OF SECURITY

Milen KISYOV, PhD
LTC, dipl. Eng, Chief Assistant in Department Operational Art, Faculty of National Security and Defence, Rakovski National Defence College, Sofia, Bulgaria
E-mail: latin001@mail.bg

Abstract: *This article looks at commitments to NATO operations consistently emphasizing the interdependence and interaction between military and non-military contributors to solving the crisis and improving security conditions. Often, the non-military contributions can best address the underlying causes of conflict and help prevent the recurrence of instability. Given such interdependent operating environment, communication and interaction between military and non-military actors are important to achieve a broader and holistic approach, in close cooperation with interested if necessary, influential interacting non-military actors.*

Key Words: *CIMIC, Civil–Military cooperation, interaction, coordination, dimension; operational environment.*

Introduction

The emergence and development of crisis and favorable conditions for solving them is always subject to various political considerations and dynamics. The countries participating in NATO enable interactions that occur in the early stages of crisis management as part of its focus on interaction for building trust and mutual understanding between international actors, including developing ways to more good cooperation.

Practical interaction and cooperation with NATO countries outside the organization, as well as local and international organizations, has significantly progressed. The intense experience and cooperation in response to the crisis led NATO and other organizations to cohesion more than ever. International organizations invite each other to participate in training and their staffs informally and often consult each other, both in terms of operations and in the development of policy and doctrine. Moreover, these international organizations put for discussion a question for the increasing importance of the essential role in domestic law and civil society in terms of stability and in crisis resolution. The diverse range of national governments and international organizations are now looking to create or strengthen the comprehensive approach to crisis management, to change conditions and to refine security.

Participation of Alliance military forces in the operations will help to prevent crises, manage conflicts and stabilize post-conflict situations together with non-military contributions from a diverse range of sources, mostly outside the Alliance. Commitments to NATO operations consistently emphasize the interdependence and interaction between military and non-military contributions to solving the crisis. Often these non-military contributions can best address the underlying causes of conflict and help prevent the recurrence of instability and disequilibrium. Given such interdependent among operating environment, communications and interaction are important for achieving a broader and holistic approach, in close cooperation with interested and influential interacting non-military actors.

The changes in the NATO Policy of the Summit 2001 reflect this significant progress and interdependent environments. It includes specific tasks to improve the consistent application of tools for crisis management in NATO, as well as dialogue and, as far as possible, *practical cooperation* at all levels with relevant international organizations (IOs), non-governmental organizations (NGOs) and local authorities in planning and implementation of operations. These specific tasks and conditions in the operational environment require the military authorities and personnel of NATO to be prepared to work with non-military actors and concepts. It should also promote mutual understanding and respect for the autonomy of decision, the relevant powers, restrictions, mandates and roles of relevant stakeholders. Therefore, the NATO military authorities should work effective and take into account non-NATO actors, their capabilities, easier access and financial opportunities.

1. Comparative analysis of joint capabilities of civil-military dimensions

Due to the asymmetry of the conflicts, the interaction between soldiers and the local population became inevitable. Military forces are now operating in a complicated environment where the distinction between battlefield and relatively peaceful area beyond is blurred. NATO operations are conducted in an environment where "the people in the streets, and houses and fields – all the people anywhere – are the battlefield"[1]

The operational environment of military mission is complex and the challenges within are interlinked. Modern crisis management operations have expanded in terms of the tasks involved. The armed forces are only one part of the comprehensive approach and therefore they are not able to address all the aspects alone. They are not equipped or adequate for performing tasks related with civil dimensions of security. In order to achieve the satisfactory end state, they need the assistance of civilian agencies to fill the humanitarian gap[2]. The accomplishment of comparative analysis is made in order to identify and distinguish the aspects and interrelationships of CMI and CIMIC in the contemporary security environment.

Civil-Military Interaction (CMI) is a group of activities based on communication, planning and coordination, shared by all NATO military authorities and conducted with international and local non-military actors during NATO operations and preparation for them, which increases the effectiveness and efficiency of their actions in response to crises.

Civil-Military Cooperation (CIMIC) is a joint function, including a set of integrated capabilities to help in achieving the mission objectives and to allow NATO to participate effectively in a wide range of CMI with various non-military actors[3] in the field at operational-tactical level.

In the CMI definition the terms "communication, planning and coordination" seems too narrow when are affected practical efforts - eg. dirrect assistance for the population. However, "based on" provide sufficient space for including these and similar aspects:

- Although this is just expression, according to which all levels of military command is added "CMI includes all military functions and disciplines."
- CMI is not military property or military controlled process, but it is definitely centered process between all types of actors (by analogy with the comprehensive approach), encouraging all parties to be involved. Overcoming the limitations of previous definition of CIMIC ("supporting the mission" - actually only teleological (target caused intentional proof), CMI is explicitly referred to as *constant activity*.

[1] *AJP 3.4.9,* 2013.
[2] *CIMIC Field Handbook, 2012:* pp. I-2-1 –I-2-2.
[3] *New definition – MC 0411/2 NATO Military Policy on Civil-Military Cooperation (CIMIC) and Civil-Military Interaction (CMI),* 2014

- Balanced view allows and gives all participants to achieve their missions as equally requiring everyone to be more flexible in planning and implementation in order all to have the same topportunity either with non-interference or help. While there is clearly expressed, it can be read as "process" - a series of activities related to each other and supporting each another capabilities.

The combination in the definition for CIMIC as "... joint function" and "set of capabilities" refers to specialized personnel staffs, affects with more results from field units operating in the area. This is hardly than the expression of the status quo, but it is essential meaning for balancing to these terms against its full integration and depersonalization in CIMIC.

Unlike the definition of CMI the focus here is on the military mission (possibly including tasks mainly for cooperation with non-military actors). This potential mismatch can be determined by observing the success of the other participants as equally supported the general perspective on the objectives of the international community.

"NATO commands" should not be misinterpreted as equal to "headquarters". AAP-6[4] defines them as "division, groups of units, organization or area under the authority of one person." Therefore, it includes all military units to squad level. "Participates …with" reiterates "sharing and carried out with" the definition of CMI.

CIMIC*, according to the new definition,* is no longer function to achieve the results observed by other military functions and disciplines rather independent from the main military activity, namely in combat actions. Therefore, by applying CMI, *may be increased the importance of CIMIC,* as its moving closer to the center of attention (focus of attention). Now it is mostly associated with allowing NATO commander to participate in CMI. However, this does not mean that traditional activities of Civil-Military Cooperation are becoming irrelevant. This shows that these activities *actually provide a foundation* for further participation in CMI. Therefore staffs/assets for Civil-Military Cooperation have to strengthen their consulting and advices to other military functions and disciplines involved in CMI. This is paramount which address the potential consequences of the planned military operations affecting non-military actors. Similarly, these inherent principles seek adequate attention of planned and ongoing actions by non-military actors to consider in the military planning and conducting of actions/operations. Based on common values of individual liberty, democracy, human rights and the rule of law, and because the common essential and enduring purpose is to safeguard the freedom and security of civil society. These values and objectives are universal and perpetual, and defending them through unity, solidarity and strength, it can be a way to find workable solutions in security and successful and effective work for CIMIC community.

When we try to analize working environment of CMI and CIMIC, the possible way for this is to understand that *capacity building and inputs are an important aspect* in all activities in operations, especially for nations and their participation in the development of capabilities. The expected impact on the development of these joint capabilities is as follows:

- Civil-Military Interaction is evaluated *as critical* and facilitates all military activities and operations, it is necessary that all doctrines have to consider and provide deductions for interaction with non-military actors and within multinational military formations in all areas of interaction;

- Institutional Cooperation (IC) requires broad policy and doctrine for domestic Civil-Military Interaction, which covers various tools in planning in emergency situations with the military doctrine of NATO.

[4] AAP 6- NATO glossary of terms and definitions, 2008.

- Effective organizational practices improve achieving universal arrangement of tasks, responsibilities and structures within multinational military formation;

- Education and training require discussion of attracting capable and adaptable players and actors according to the efforts. When and where possible, the external experts on various issues must participate and contribute to the education and training based on relevant and well-developed training modules;

- Materials, platforms and instruments that facilitate Interaction with relevant external actors will need not only further development and delivery, but also obtaining, acquisition and specialized analyses;

- Permanent and timely access of CIMIC specialists to wide list of non-military expertise for *interaction and coordination*. Otherwise, without that can be overwhelmed overall working process and requires some time to take on new responsibilities and acquire new abilities;

- Politico-military advice on high level planning and decision-making will ensure a wider interaction;

- Improved work with centers of information as centers of knowledge will support the comprehensive efforts including these of Civil-Military Cooperation;

- The requirement for increased information sharing at all levels can inevitably cause a revision of the current arrangements for safety and security of information, data and protocols established standard operating procedures;

On the other hand, the most important operational capabilities for CIMIC (in brackets) definite to perform the basic functions and tasks in multinational operations, according to perceptions of NATO are:

- The ability to effectively influence over hostile forces (effectiveness);
- Maneuverability and mobility (deployability);
- Protection of forces and infrastructure (survivability);
- Resilience and flexibility (sustainability);
- Compatibility including with partner countries. (interoperability).

Examined these two aspects of civil-military dimensions contain these abilities, which lead to the conclusion that together they can increase the effectiveness of implementation of the tasks set before them.

2. Analysis of features and contributions of CMI and CIMIC to comprehensive approach for the security

After analyzing the working environment, capabilities for impacts of the two aspects of civil-military dimension for security is need to be presented features of civil military dimensions. It will help for development of understanding how CMI and CIMIC depict and identified the most important drawbacks and challenges in front of security.

Moreover, as the Strategic Concept states, NATO's experiences and lessons learned from past and ongoing operations show that to conduct an effective crisis management there is a need for a comprehensive political, civilian and military approach. Therefore the Alliance will actively encourage collaborative analysis, planning and conduct of military operations. This will allow maximising coherence and effectiveness of the NATO and EU approach towards civil-military relations.

The purpose of CIMIC is to establish and maintain on the one hand the cooperation between the military components and any external civilian actors including IO and/or NGO who's in theatre efforts are mutually supportive. On the other hand CIMIC should establish and maintain the cooperation with the civilian authorities and populations within the Commander's area of operations, in order to create the best possible moral, material and

tactical conditions for achievement of the mission's purpose. The focus of CIMIC is to support the military mission.[5]

CIMIC, successfully implemented in NATO operations are useful in the full range - from combat operations through peacekeeping operations up to disaster reliefe. The advantage for this is improving and facilitation of the conditions in a humanitarian disaster and crises. Essential for successful implementation and management of CIMIC activities is the establishment and maintenance of a reliable relationship with organizations working for the civil sector. *This relationship forms a solid basis* and can be effective only through constant, active and effective cooperation and interaction. The reason is the fact that civilian organizations perform a wide range of activities covering humanitarian assistance, human rights, protection of small groups and population, help for refugees and displaced persons, legal assistance, medical care, reconstruction, agriculture, education, art, science and general financial planning.

Joint planning and close working relationships (supported CMI and CIMIC) between the military and appropriate civil organizations and agencies will be required before and during a military deployment and subsequently during sustainment of military operations. These relationships will be conducted both inside and outside the Operational area (OA) and at any level of command when military planning takes place. It must be recognized, however, that even when such relationships or planning mechanisms exist, it may not always be possible to conduct them on a formal basis.

Based on analysis of operations in the last 15-20 years it is possible to identify some common and important operational capabilities for the participation of forces in multinational operations:

- Strike capabilities – opportunity be defeated proven hostile parties and their bases;
- Maneuvering capabilities, including the ability to relocate to and within the area of operation;
- Capability to act in multinational environment – this requires adaptability of doctrines, procedures and staffs – interoperability;
- Capability for CIMIC (and CMI) – trained personnel to work in interaction with non-military actors in the area of operation.

For all these different directions and varieties of efforts and actions (characterized *Civil-Military Dimension*), the staffs and CIMIC assets must fully understand the mandate, role, structure, work methods and principles of partner and/or opposite organizations.

The commanders in contemporary operations must have sufficient amount of money and other resourses not only for CIMIC activities but also for creation and development of effectively CMI to conduct effective support to the operations. In these resourses include also and assets - staffs elements (teams) and functional specialists. Staff has to take into acount conceptual and planning role of CIMIC in general planning. Activities in this area could include a wide variety of techniques depending on the situation, mandate and available forces and means, such as:

- *Relationship* with civilian organizations at grassroots level;
- Preparation of *regular and continuous assessments* of the needs of the civilian population, to determine any need and how it could be satisfied;
- Participation in the decision making process of commanders and provision of implementation of the plan in execution;
- Management of the current situation analysis of civilian and quantifying the difficulties and its impact over military operations;
- Participation in integrated planning with civilian agencies;

[5] EU Concept for Civil-Military Co-operation(CIMIC) for EU- led Military Operations, 2009.

- Work for the timely and smoothly transfer of responsibilities to international and local civic authorities.

CIMIC branches/sections/teams/specialists actually managed CIMIC operations in support all military and non-military activities. They can:

- To engage in contacts with capacities in definite area;
- To engage in support of tactical teams;
- Be part of CIMIC team/platoon/company/group/;
- To work in CIMIC center.

Their work could include activities from field of Civil-Military interaction with NGOs and local authorities through:

- Providing and renewal of assessments;
- Maintenance of Humanitarian Aid;
- Coordination of small projects in the area of responsibility;
- Management of people and resources needed to maintain normal living conditions;
- Gathering information on indicators for normalization of society a fullfil nd efficiency measures.

This is essential that these two aspects of Civil-Military Dimension are still made of the same composition build by CIMIC specialists.

It is through this close *Interaction* and *Reconciliation* of CIMIC and CMI principles and functions can be achieved a wide range, ability and activities of mutual interest. As a minimum, when parallel CMI and CIMIC activities have to be conducted, an overview of civilian plans and activities will have to be maintained.

On the other hand, conducting of CIMIC planning and involvement, we have to remember that CIMIC implies neither military control over civil organizations or agencies nor the reverse. Normally the military will be responsible only for security related tasks and for support to the appropriate civil authority. In exceptional circumstances, the military may be required to take on tasks, which are normally the responsibility of a civil authority, organization or agency. These tasks should only be taken on when the appropriate civil body is not present or is unable to carry out its mandate and when an otherwise unacceptable vacuum would arise. The military will often require access to local civil resources. In such circumstances every effort will be made to avoid adverse impact on local populations, economies, infrastructure or the work of civilian organizations. There is normal position where CMI can be used to fulfil some special tasks as negotiaions and mediation.

The military should be prepared to undertake, when requested by the legal or recognized civil authority and approved by the commander, such tasks necessary to maintain momentum towards a lasting solution to the crisis until the mandated civil authority, organization, or agency is able to assume them. Responsibility for civil-related tasks and some parts from civil emergency planning will be handed over to the appropriate civil authority, organization, or agency as soon as is practical and in a smooth manner as possible.

Therefore, CIMIC planning must:

a. Adhere to the overall military mission, helping to maximize the non-military contribution in achieving a stable security environment while minimizing potential for further conflict.

b. Support the establishment and maintenance of relations with all potential civil partners. Appropriate liaison arrangements will be critical to this effort.

c. Ensure that any activities conducted in support of the civil environment are necessary, agreed with the appropriate civil authority, can be resourced, and follow a strict line of operation. CIMIC and CMI activities in support of the civil environment should only be implemented when these preconditions are in place.

Conclusion

NATO forces involved in evolving environment of Civil-Military Interaction must have ability to meet these requirements and capabilities described above, to implement NATO's contribution to comprehensive approach by the international community in order to increase both the effectiveness and efficiency in response to the crisis.

That is reason why CMI in NATO's involvement includes all military functions and disciplines that have to be harmonized with appropriate process approved by and assisting commanders and facilitate/support the special abilities of Civil-Military Cooperation. These capabilities can and must be adapted to the new framework and further development for building new general policy and concept. This policy aims to increase military NATO contribution for crisis response. This can be achieved by improving NATO military-like ability to interact at the appropriate levels with non-military actors and use abilities of NATO's Civil-Military Cooperation.

Mutual reinforcement and sustainability of strategic partnerships in NATO should be further strengthened at all levels. All activities related to other international organizations and non-governmental organizations have to be in accordance with the action plan for comprehensive approach.

But only the future will shows whether it is appropriate to separate these two functions of Civil-Military Dimensions, whether the same assets must fulfill them and whether it will affect the performance of CIMIC tasks.

Civil-military cooperation as a military facilitator and a certain type of culture of cooperation has to be mainstreamed into structures of NATO and EU. On the strategic level, both organisations created special cells and arrangements serving the implementation of CIMIC and supporting Civil Dimention of Security. As to the operational and tactical level, it is impossible to predetermine the shape of civil-military coordination structures, as they have to be individually tailored to each mission.

As a final point, it is necessary to state that the biggest issues con-cerning the implementation of civil-military cooperation and coordination in the field come from lack of will and lack of information sharing. CIMIC is therefore very much dependant on the personal skills of individual operators. Careful choice of personnel and their scrupulous training could enhance the effectiveness and ability to perform successful civil-military cooperation, even if it is not the answer to all concerns.

CIMIC as a military function that is an integral part of modern multidimensional operations, addresses all cooperating parties within a conflict situation and facilitates mutual support of civilian capabilities to military forces and vice versa. The governing idea in all those interactions is reaching the defined and commonly desired end state, for the best of the local population, the civil actors and the Alliance, which will be, under the best of circumstances, hard to achieve.

Today`s comprehensive and crucial agenda for NATO adaptation is performed to face combined challenges for nations in the East and in the South. The demonstrated cohesion and resolve, as well as commitment to the transatlantic bond, must continue to guide the response.

BIBLIOGRAPHY:

1. AAP 6- NATO glossary of terms and definitions, 2008.
2. Active Engagement, Modern Defence-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, 2010.
3. AJP 3.4.9 - Allied Joint Doctrine for Civil-Military Cooperation, edition A, version 1, 2013.
4. MC 0411/2 NATO Military Policy on Civil-Military Cooperation (CIMIC) and Civil-Military Interaction (CMI), 2014
5. CIMIC Field Handbook, 3rd edition, Version 3.0.0, Civil-Military Cooperation Centre of Excellence, 2012.
6. EU Concept for Civil-Military Co-operation(CIMIC) for EU-led Military Operations, 2009.
7. Marinov, Ivo; Kisyov, M., Essence, functions and tasks of CIMIC bodies and assets, lection in CIMIC in multinational operations course, Rakovski National Defence College
8. Marinov, Ivo; Kisyov, Milen, Working environment for CIMIC, lection in CIMIC in multinational operations course, Rakovski National Defence College

COMPLEXITY IN THE SECURITY ENVIRONMENT

Florina Daniela GHEORGHE
PhD student in „Intelligence and National Security" at „Mihai Viteazul" National Intelligence Academy, Bucharest, Romania, ghe_florina@yahoo.com

Abstract: *International security environment has undergone further transformation, becoming extremely volatile through the amplification of non-state actors and international manifestations of segregation. Therefore, the old paradigms that used to explain the international framework have been increasingly challenged or weak. Against this background, in recent years, International Relations theorists advanced the idea of „chaos" and „new anarchy in the system", the security environment being known under the abbreviation of „VUCA" (volatile, uncertain, complex, ambiguous). This paper proposes a new approach provided by the complexity theory: to highlight new concepts for analyzing the international system throughout the use of models meant to measure the nonlinear dynamic behavior of complex systems order.*

Keywords**:** *security environment, chaos, complexity, nonlinear dynamic behavior.*

Introduction

We live in a century marked of pendency, evolutions and fast transformations, manifested both at individual level, and mostly at social/ organizational level. Thus, the security environment does not compromise from these considerations. The amplification of the non-state actors, the segregation manifestations and the ascension of the religious fanaticism make us assist, more and more, to the world's division. As Robert Cooper[1] highlighted, „nowadays we have, first, a premodern world characterized by pre-statehood and post imperial chaos".

It becomes more obvious that we cannot report anymore to the security environment through the angle of the old paradigms. The terrorist attacks from September 11, the annexation of Crimea by the Russian Federation and the appearance of the Islamic State (to offer only few examples) have, no more, nothing in common with the principles of the power equilibrium/ balance that governed the International Relation until recently.

The international medium is a *complex adaptable system* in which little changes of the initial conditions and the further interventions of any dimension can take to disproportionately high effects or as Nassim Nicholas Taleb calls them „black swans", these having three major attributes: rarity, external impact and retrospective predictability[2].

A *complex adaptive system* appears when the environment is instable, but not completely chaotic. The stable environments lead to systems in balance, which most probably will not adapt to major changes. In the chaotic environments, the systems cannot find productive patterns. At the edge of the chaos – a good analogy with the current social transformations – can appear innovating and dramatic changes in the patterns' activity and the

[1]Robert COOPER, *The Breaking of Nations: Order and Chaos in the Twenty-First Century*, Bucureşti: Editura Univers Enciclopedic, 2007, p. 42.
[2]Nassim Nicholas TALEB, *The Black Swan: The Impact of the Highly Improbable*. Bucureşti: Editura Curtea Veche, 2010, p. 16.

systems can move to higher levels of performance. Such innovations, however, depend on the information flows through the interconnected networks[3].

1. Considerations concerning the security

Along the time, theorists of International Relations phrased a multitude of definitions of the *security concept*, without being able to find a consensus regarding this subject.

In antiquity, the term „security" was understood in the sense of „liberty in the face of threatening". This formulation is presented also in the definition that Arnold Wolfers[4] gave, according to which „the security, in objective sense, measures the absence of the threats regarding the obtained values, and in a subjective sense, the absence of the fear that such values would be attacked". The pyramid of Abraham Maslow, that situates the security on the second place, after the primary needs, seems to fit in this concept.

As noticed, Arnold Wolfers outlined the existence of some objective and subjective components of the national interests, and of the threats to which these are subject. Thereby, the politics that are to be adopted by the states in view of assuring the security will be defined depending on the identified national interests and on the threats at their address.

On the other hand, the realist current sets forth that the fundamental objective of any state is its own survival. According to Kenneth Waltz theory[5], „in anarchy, the survival is the highest objective. The states can search to meet other objectives as peace, the benefit or the power only if the survival is assured".

A state's security generically refers to the lack of the threats to the territorial independence and integrity, as to its capacity to defend them.

In the center of the debate regarding the security it is the state, thanks to its sovereign character, but we must take into account the fact that we are crossing a century in which the state can no longer be analyzed as topic by itself, but through its relations and interdependent with other actors of the system. History has proved, not once, that a state cannot assure, in an absolute way, its security by itself.

Barry Buzan introduced in the literature the term *regional security complex*, representing „a group of states whose major security preoccupations cannot be treated efficiently separated". [6] Unlike the regional security subsystem and the subordinated system, which are ways of treating together regarding a single criteria some states that are geographical close call, the security complex brings in foreground the question of a significant interdependence existence between participants. In the same context, is developed the idea that these interdependencies are not solely military, diplomatic or political, being able to manifest in a social level, as well as in the economic domain or in environment security matters[7].

---

[3]Judith E, INNER, David E. BOOHER, *Consensus Building and complex adaptive systems: A framework for evaluating collaborative planning*, Journal of the American Planning Association, fall 1999, Vol. 65, No.4, p. 412.

[4]Arnold WOLFERS, *„National Security" as an Ambitious Symbol*, Political Science Quarterly, 1952, 67 <4>, p. 485.

[5] Kenneth WALTZ, *Theory of International Politics*, McGraw-Hill, Boston, 1979

[6]Barry BUZAN, *People, States and Fear: An Agenda for International Security Studies in the Post Cold War Era,* Cartier: Chişinău. Cap.I, II, III, IV, 2000, p. 106.

[7] BUZAN, *People, States and Fear ,* p. 106.

2. From constructivism to complexity

The constructivism represents one of the most innovating thinking currents in the International Relations, the most frequent name associated to this theory being the one of Alexander Wendt. For constructivism, the world of interactions between the international actors is, eminently, a social space. The international system is a social creation in its ensemble, just as its defining components – more exactly, the processes, the actors and the international structures – are social products. One of the essential premises of the constructivism is that the material factors that are present in the international relations (theories, distances, military capacity, and natural resources) do not signify anything in the absence of some *complex social processes* through which is assigned a certain sense[8].

Complexity theory is predominantly present in the social sciences and informatics, Mark McElroy[9] saying that it is a „reliable solution in search of unorthodox problems, providing an explanation of the meanings in which the living systems are engaged in adaptive learning". On the other hand, Ortegon-Monroy[10] and Smith and Humphries[11] concluded that complexity theory is difficult to translate into practice.

Massimo Pigliucci[12] states that a key figure in the development of modern science was Rene Descartes, a french philosopher who held that the idea of *complex systems* can be understood by analyzing each part in turn[13], then putting all the pieces together to get a comprehensive picture (reductionism theory). Pigliucci calls into question this approach, highlighting the potential of altering the properties of the separation so much that what we've learned from studying the separate pieces can induce a different and wrong idea on the system as a whole: „Reductionist science can study the emergent properties which, by definition, are the result of complex interactions?" He gives the example of the interaction between hydrogen and oxygen resulting in water. Pigliucci states that, knowing everything about the structure and behavior of atoms that make up water, allows us to predict the structure but not the behavior of water. *Complexity produce new specific properties in the new level of the organization, which are not the result of sum parties, but of their interactions.*

He also connects the two theories, noting that complexity theory is derived from chaos theory, hence the phrase „chaoplexity". Chaos refers to a deterministic phenomenon (not by chance/ random) characterized by special properties that makes the predictability of its occurrence very difficult. An erratic behavior is one that although it is not produced random it appears as a series of random occurrences. Chaotic dynamics are usually, but not always, the prerogative of nonlinear systems. Not all systems generate nonlinear chaotic behavior! Starting from the Edward Lorenz's „butterfly effect", Pigliucci states that the technical term for this phenomenon is „sensitivity to initial conditions" („SCI"), meaning that a small perturbation of the system can cause a number of effects that lead, ultimately, the macroscopic consequences.

Piglicci also points out that we can think of complexity theory as an attempt to study systems that meet two conditions: 1) are made up of many parts that interact and 2)

---

[8]Alexander WENDT, *Constructing International Politics*, International Security, 20 (1), summer of 1995

[9]Mark W. McELROY, *Integrating Complexity Theory, Knowledge Management and Organizational Learning*, Journal of Knowledge Management, Vol. 4 No. 3, 2000, pp. 195-203.

[10] Maria Carolina ORTEGON-MONROY, *Chaos and Complexity Theory in Management: An Exploration from a Critical Systems Thinking Perspective*, Systems Research and Behavioral Science, Vol. 20 No. 5, 2003, pp. 387-400.

[11]Aaron SMITH, Clare HUMPHRIES, *Complexity Theory as a Practical Management Tool: A Critical Evaluation*, Organization Management Journal, Vol. 1 No. 2, 2004, pp. 91-106.

[12]Massimo PIGLIUCCI, *Chaos & Complexity. Should We Be Skeptical?*, Skeptic Magazine, Altadena, California/ SUA, Vol. 8 No. 3, 2000., pp. 62-70.

[13] For a clearer overview of the approach, read the word on the meaning of „state"

interactions result in emergent properties that are not readily reducible to a simple sum of properties of individual components.

Complexity theory uses models to measure the nonlinear dynamic behavior of complex systems order.

Phil Anderson[14] believes that new properties come to dominate the behavior of the system as we grow and introduce a degree of freedom to break the symmetry parameter. Components of a system interact. Increasing the number of interactions or certain interactions over others (symmetry breaking), triggers feedback loops among the components that lead to collective behavior. Components that are blocked in such behavior can be treated together as a new unit.

While the composition of a system remained the same, its internal borders - which suggests how to analyze a system in „parts" - have been redesigned from the inside. Complex systems are often organizations formed from many heterogeneous parts that interact locally, in the absence of centralized control peace maker.

In nonlinear systems, small changes in the causal elements over time does not necessarily produce small changes in other specific aspects of the system or characteristics of the system as a whole. Both can change very much indeed, and in addition, they may change in ways that do not involve just one possible outcome.

Pavard and Dugdale[15] synthesized the following properties of complexity:

a) non-determinism and non-tractability. It is impossible to anticipate precisely the behavior of complex systems, even if we completely know the functions of its constituents. The behavior of these systems is not random in the sense of chaotic; they operate by feedback effects and is unlikely to be detected by standard measurements or by combination of assumed determinants and alleged effects.

b) limited functional decomposability. A complex system has a dynamic structure. Therefore, it is difficult, if not impossible, to study its properties by decomposing it into functionally stable parts. Constant interaction with the environment and self-organization properties allow restructure itself.

c) distributed nature of information and representation. A complex system possesses properties comparable to distributed systems (in a connectionist meaning); thus some features may not be located accurately. In addition, relationships between elements of the systems may be complex and may contain short-range feedback loops (both positive and negative).

d) emergence and self-organization. A complex system include emergent properties that are not directly accessible (or looking identifiable) by understanding its components.

Thus, while complexity as an area of study circumventing distinctive rigorous definition, we can say on a general level that complex systems are those systems „whose global behavior tends to/ lead to structural models and dynamic multi-scale". An important property of complex systems is how it has a self-organizing behaviour, led by coevolutionary interactions.

[14] Philip.W. ANDERSON, *More is Different*. Science, 177:393:396, 1972

[15]Bernard PAVARD, Julie DUGDALE, *The Contribution of Complexity Theory to the Study of Sociotechnical Cooperative Systems*, available athttp://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.129.70&rep=rep1&type=pdf, accessed at 15.03.2015

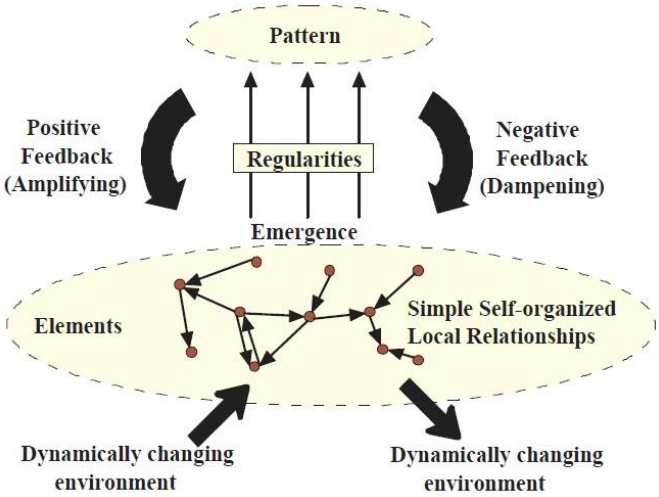


Figure no. 1. Complex adaptive system [Antoniou, Pitsillides 2007]

3. Complexity and the security environment

Neil E. Harrison, who analyzed international relations through the theory of complexity, observed that current theories tend to rely on social models (realism, for example, that sees political behavior being driven by essential human characteristics within fixed structures). *Complexity theory sees world politics as self-organising complex system in wich macroproperties emerge from microinteractions*. Harrison classified the state as an open system to other natural and social systems, as it has access to technological, cultural and economic systems that influence political elections. The state is also influenced by other states and numerous cross-border interactions between large corporations, NGOs, terrorist groups, etc. In such complex systems is almost impossible to follow linear causal links[16].

In different contexts, the same question can lead to different results, and this can not be predicted by simplistic models of international systems. Since interactions affect each other in social systems, when looking for causes of observed effects it is necessary to look rather to the evolution of the system instead of notice a single event. Complexity theory focuses precisely on the processes and relationships between components, not at the system components themselves.

Harrison found that application of complexity theory can represent a gain in world politics: *„This ontological shift from simple to complex systems opens new paths to knowledge and understanding yet incorporates much current knowledge; it validates novel research methods; and theories founded in this approach will generate radically different solutions to policy problems."*[17].

Complexity is present then, or rather more so then, when it comes to conflicts. In regard, Peter Coleman noticed a „paradox". In his opinion conflicts are „essentially stable despite the extraordinary volatility and change".

„If we consider the conflict in the Middle East for example, it appears by most accounts intransigent; with a past, present, and future cloaked in hate, violence, and despair. Yet, over the years we have also seen major changes in important aspects of the conflict such as in leadership, policy, regional circumstances, intensification and de-escalation of violence, intragroup divisions, popular sentiment, and international intervention strategies. In other words, we have seen extraordinary changes occur within a context of a pattern of stable

[16]Neil E. HARRISON, *Complex Systems and the Practice of World Politics*, in Neil E. HARRISON (ed.), *Complexity in World Politics, Concepts and Methods of a New Paradigm*, State University of New York, 2006, p. 8

[17]HARRISON, *Complex Systems and the Practice of World Politics*, p. 2.

destructive relations. This paradox of stability amidst change is evident in intractable conflicts at all levels, from estranged siblings and neighbors to warring ethnopolitical factions. They are at once frozen, unyielding, often persisting in hostile states for generations, yet they are also some of the most volatile and dynamic social processes on earth"[18].

International Centre for Conflict and Complexity at the University of Warsaw brings complexity theory to conflict research, with a strong emphasis on socio-psychological aspects of it. The ICCC researchers characterized *intractable conflicts as complex, nonlinear systems* – sustained in a state of destructiveness by a variety of emergent, embeded and automatic processes. In their opinion, *„viewing conflict at a single point in time, or focusing on a single aspect, was ultimately problematic because it failed to capture the fact that conflict, particularly intractable conflict, is multifaceted; involving multiple experiences and encounters between many different parties over a variety of issues under diverse conditions at different points in time."*[19]

Also, according to Harrison, the environment affects the behavior of the system in two ways. First, it constrains what is possible and ―selects behaviours that are most appropriate within current institutional arrangements. Second, perceptions of environment influence agent's internal models.[20]

With a vast experience in intelligence, Dr. Gregory F. Treverton addressed the complexity from a new and interesting angle. In an article which was integrated in an intelligence and national security project developed by the RAND Center for the Study of Asymmetric Threats, elaborated for the Swedish Agency for Emergency Management[21], Treverton characterize the „complexities" as a new category of intelligence problems, being present, in particular, to assess terrorist groups, thereby protecting national security. What is even more interesting, is the comparison made between „mysteries" and „complexities", the major difference being that the first one has some shape; we know what variables matter most in producing an outcome and we may have some historical evidence about how they interact. By comparison, in complexity, large numbers of relatively small actors respond to a shifting set of situational factors. Thus, they do not necessarily repeat in any known/ established pattern and are not amenable to predictive analysis. These characteristics describe many transnational targets, like terrorists - small groups forming and reforming, seeking for vulnerabilities, thus adapting constantly and interacting in ways that may be new.

In complexity, uncertainty is very high and difficult to reduce, because we do not know exactly what factors are most important, nor how they interact. The 9/11 event transformed the old belief that „they (meaning the actors that threaten national security) could not or would not" to „*anything* can happen". Treverton emphasizes the need to import new concepts and to consider new models and theories to solve the challenge of terrorism seen in terms of complexity.

Reviewing a number of characteristics of terrorism, he actually describes largely complexity:

- Terrorism is predominantly a phenomenon of group psichology, where a social system of sympathizers and supporters exerts multiple influences on individual behavior;
- There is not singe root cause of terrorism, rather there are multiple paths to terrorism;

---

[18]Peter T. COLEMAN, Robin VALLACHER, Martin NOVAK, Lan BUI-WRZOSINSKA, *Intractable Conflict as an Attractor: Presenting a Dynamical Model of Conflict, Escalation and Intractability*, American Behavioral Scientist, 2007, vol. 50, p. 2.

[19]Diane HENDRICK, *Complexity Theory and Conflict Transformation: An Exploration of Potential and Implications*, Working Paper 17, University of Bradford, Centre for Conflict Resolution, Department of Peace Studies, june 2009, p. 26.

[20] HARRISON, *Complex Systems and the Practice of World Politics*, p. 35.

[21] Gregory F. TREVERTON, *Adressing „Complexities" in Homeland Security*, The Swedish National Defense College, 2009.

- Terrorist groups and their supporting social systems are embedded within evolving institutional and political structures and complex religious belief systems;
- Terrorist actions have several, perhaps many, audience, and evolve with responses by those audiences;
- Terrorist innovate and adapt in response to changes in both counterterrorism measures and independent events;
- Self-organizing terrorist groups form primarily throught social networks; as such their structure is largely a function of those social ties;
- Descentralized terrorist networks facilitate resiliency in operations, diffusion of idealogy and innovation, and distribution of resources and information.

Conclusions

Although a „school of thought" regarding complexity in security science/ international relations is not yet emerged, a series of concepts begin to develope, especially in terms of a new approach to intelligence analysis.

The complexity is still quite disputed among analysts that use predictive models, as uncertainty introduced into the equation can not generate predictions for the next 50 years, as we would like. Challenging this approach derives much more from the lack of development in elaborating a methodology and clearer definitions of used terms. Thus, regarding the applicability of complexity in the international security environment, the scientific community has only agreed on terms such as „self-organization" and „resilience", common to all sciences using complexity theory.

The advantage of complexity is given precisely by its transdisciplinarity, especially considering the fact that we live in a world of interdependence and coagulation circumvention interests.

BIBLIOGRAPHY:

1. ANDERSON, Philip.W., *More is Different*. Science, 177:393:396, 1972.
2. BUZAN, Barry, *People, States and Fear: An Agenda for International Security Studies in the Post Cold War Era,* Chişinău: Cartier. Cap.I, II, III, IV, 2000.
3. COLEMAN, Peter T., VALLACHER, Robin, NOVAK, Martin, BUI-WRZOSINSKA, Lan, *Intractable Conflict as an Attractor: Presenting a Dynamical Model of Conflict, Escalation and Intractability*, American Behavioral Scientist, 2007, Vol. 50.
4. COOPER, Robert, *The Breaking of Nations: Order and Chaos in the Twenty-First Century*, Bucureşti: Editura Univers Enciclopedic, 2007.
5. FONTANA, Walter, BALLATI, Susan, *Complexity; Introduction to Issues in and about „Complexity"*, presented at the seminary „Philanthropy and Social Change", New Jersey: Robert Wood Johnson Foundation, Princeton, 15 october 1998.
6. HARRISON, Neil E., *Complex Systems and the Practice of World Politics*, in HARRISON, Neil E. (ed.), *Complexity in World Politics, Concepts and Methods of a New Paradigm*, State University of New York, 2006.
7. HENDRICK, Diane, *Complexity Theory and Conflict Transformation: An Exploration of Potential and Implications*, Working Paper 17, University of Bradford, Centre for Conflict Resolution, Department of Peace Studies, iunie 2009.

8. INNER, Judith E, BOOHER, David E. , *Consensus Building and Complex Adaptive Systems: A Framework for Evaluating Collaborative Planning*, Journal of the American Planning Association, Vol. 65, No.4, fall 1999.
9. McELROY, Mark W., *Integrating Complexity Theory, Knowledge Management and Organizational Learning*, Journal of Knowledge Management, Vol. 4 No. 3, 2000.
10. ORTEGON-MONROY, Maria Carolina, *Chaos and Complexity Theory in Management: An Exploration from a Critical Systems Thinking Perspective*, Systems Research and Behavioral Science, Vol. 20 No. 5, 2003.
11. PARROTT, Lael, KOK, Robert, *Incorporating Complexity in Ecosystem Modelling*, Complexity International, Vol. 7, 2000.
12. PAVARD, Bernard, DUGDALE, Julie, *The Contribution of Complexity Theory to the Study of Sociotechnical Cooperative Systems*, available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.129.70&rep=rep1&type=pdf.
13. PIGLIUCCI, Massimo, *Chaos & Complexity. Should We Be Skeptical?*, California: Skeptic Magazine, Vol. 8 No. 3, 2000.
14. SMITH, Aaron, HUMPHRIES, Clare, *Complexity Theory as a Practical Management Tool: A Critical Evaluation*, Organization Management Journal, Vol. 1 No. 2, 2004.
15. TALEB, Nassim Nicholas, *The Black Swan: The Impact of the Highly Improbable*, Bucureşti: Editura Curtea Veche, 2010.
16. TREVERTON, Gregory F., *Adressing „Complexities" in Homeland Security*, The Swedish National Defense College, 2009.
17. WALTZ, Kenneth, *Theory of International Politics*, Boston: McGraw-Hill, 1979.
18. WENDT, Alexander, *Constructing International Politics*, International Security, 20 (1), summer 1995.
19. WOLFERS, Arnold, *„National Security" as an Ambitious Symbol*, Political Science Quarterly, Vol. 67, No. 4, 1952.

COMPLEXITY DRIVEN SECURITY

Maria – Cristina MURARU
PhD student, "MIHAI VITEAZUL" National Intelligence Academy,
e-mail: cristina.muraru@gmail.com

Giorgiana – Raluca STOICA
PhD student, "MIHAI VITEAZUL" National Intelligence Academy
e-mail: ralluca.stoica@gmail.com

Abstract*: Nowadays' security environment is conceived in terms of connecting apparent isolated events, periodic trends and episodic events, after an era best described by a definition including terms such as immediate cause-and-effect phenomena, long-term tendencies, and most important, neat, orderly patterns.*

Given this shift of paradigm, one can assume that complexity theory's metaphors – a science stating that societies', states' and individuals' existence are interacting in anything but a linear and predictable manner – can be also applied in the issues concerning the security environment.

The present paper shall try to underline the old and new metaphors of both Clausewitz's chaos and The Santa Fe Institute's complexity theory ,hidden' within national security strategies and policies.

Keywords: *complexity, chaos, nonlinear, order, strategy, security, systems.*

Introduction

Relationships between states and groups of states are similar to the interactions between microscopic structures in physics: a small number of variables are required to portray the process.

When describing such events and phenomena, present day scholars and experts tend to use words such as *chaos, complexity, systems, uncertainty, emergence,* etc.

It is widely known that the paradigm of chaos was associated with battle and conflicts: Prussian general Carl Phillipp Gottlieb von Clausewitz's 'Vom Kriege' is the first military book in which one identify principles and aspects which would later be included in chaos theory. Later on, renowned scientists proposed and explained the usefulness of the chaos and complexity concepts in describing international relations and security. What they suggested was applying metaphors such as strange attractors, fractals, self - organization etc., to the military and intelligence domains.

It should be understood that a new set of principles to understand the hidden rules that determine a system or group of systems does not mean new behaviors of those systems, but a better depiction and perhaps, better interactions with those described.

1. Complexity theory

In the early 1960s scientific efforts to forecast weather were hindered by the understanding and nonetheless computing of the nonlinear, non-cause-and-effect evolution of airwaves. Edward Norton Lorenz, an American meteorologist and mathematician was the first to describe these movements using advanced mathematics and later on, during the 1980s

James Gleick's best-seller Chaos: Making a New Science popularized what we currently call Chaos Theory.

Complexity theory or Complex Adaptive Systems/ CAS theory is a relatively new science that was first brought to the scientific world's attention by the Santa Fe Institute in New Mexico. Similarly to cybernetics, systems theory and Chaos theory, Complexity theory is based on the idea of the entwined and continuous interaction and movements of both systems and their components across traditional scientific boundaries.

In other words, the ‚complexity' term which is nowadays prone to be used in order to describe tangled, complicated systems is actually associated with the intricate inter-connectivity of components within a system and between the very system and its surrounding environment[1].

Most natural systems (the human mind, ecosystems, groups), especially societies, and increasingly most artificial systems (man-made computing systems, evolutionary programs, and, the most famous of them all, the Internet) tend to be best described by complex behaviors that are a result of a large number of nonlinear interactions between another large number of system components. Given the fact that nonlinearity was until several decades referred as the Twilight Zone of mathematics, the rise of Complexity theory has paralleled the development of the computer as nonlinear behavior is extremely difficult to describe without automatic aid.

1.1 Basics

Complexity theory can be best described as the fundamental manner of investigating the very core of nonlinear systems' behavior in contrast to the non-native, mathematics based on the linear, Newtonian manner of thinking: statistics and calculus. Linear systems are the result of what we simply ‚cause-and-effect processes'. They are consistent with easily stated predictions, as a result of meticulous planning, monitoring and control, and with a direct proportionality between input and output. Also, linear systems are the epiphany of reductionism: large, convoluted systems are analyzed by reducing them to manageable wads.

Opposing stand nonlinear systems or, in better chosen words, the *ways of nature:* environments where there is more to the system than the sum of its parts, in which inputs and outputs are anything but proportional and, most important, cause and effects are not observable. In nonlinear systems phenomena are uncertain, but within bounds, and where conventional control is not a solution, but self-organization is.

CAS are dynamic systems which are able to adapt in and evolve alongside a changing environment. Also, CAS and their surrounding environments are not separable: one cannot talk about a CAS without an environment to which the system adapts. In other words, change means co-evolution with all the other systems in the environment, rather than adaptation, which in most cases leads to a fixed state, thus to the cessation of the system.

1.2 Attributes of CAS

Traditionally, the critical characteristics of a complex adaptive system are:

- *Self-organization*

When a complexity theorist hears about a complex system the first thing to come to his/her mind is self-organization. The idea of self-organization was first coined by Maturana and Varela's research on biological systems, creating the term *autopoiesis* as the internal process in which each system subpart is directly responsible for the other components' and the entire system's transformation.

[1]Vasant, HANOVAR, *Complex Adaptive Systems Group,* Iowa State University, available at http://www.cs.iastate.edu/~honavar/alife.isu.html, accessed at 23.03.2015

In regard to CAS, components of such a system, called agents, take action in proximity to and to in concert with each other, for their own reasons. A system is self-organized when it evolves into an even more complex form without being externally managed, manipulated or controlled. Because relationships between agents are almost always mutual and feedbacks are unceasing, a self-organizing system is typically nonlinear. As further described, a CAS is self-organizing through its emergent and feedback components.

- *Emergence*

The notion of emergence is based on the idea that the whole consists of greater significance than the sum of its parts. In other words, the group's or system's behavior is distinct from the sum of the agents' own actions. Through emergence, CAS determine new and coherent internal structures, patterns which, most important, were not previously detected. Emergent phenomena are perceptible on a large scale despite they are derived by small sized events.

Non-linearity plays an immense role when it comes to both self-organisation and emergence: the Newtonian paradigm, as it stated that a small input shall create a small output, was the hallmark of previous scientific research, but in current CAS theory, any small turbulence, created by the surrounding environment or by one or several agents in the system's evolution can lead to great, structure - remodeling adjustments.

- *Adaptability*

The system is open: information and energy flow in and out. New information enters the feedback cycle and further influences the behavior of individuals, thus the global demeanor of the system *adapts* to the surrounding environment.

- *Co-evolution*

This attribute is actually the evolved version of Darwinian evolution. Instead of being surrounded by a stable environment which allows the agents to slowly adapt and evolve, complex theory suggests that agents interact with other agents, who are themselves adapting and evolving.

- *Feedback*

New information enters into the feedback loops and influences the behavior of the individuals, and thus the overall behavior of the system adapts to the external environment.

- *Resilience*

It refers to the capacity of a system to absorb and utilize or even benefit from perturbations and changes that attain it, and so to persist without a qualitative change in the system's structure. In other words, complex adaptive systems are resilient as they are able to respond in a manner that allows them to redress themselves or rapidly enclose the effects of the unexpected event or deliberate perturbation.

- *Sensitivity to initial conditions*

Chaos theory tells us that non-linear developments are extremely sensitive to initial conditions: a slight difference in any variable of the state of the system from which such an evolution begins can lead to completely trajectories as the difference is deepened by positive feedbacks. Sensitivity to initial conditions is widely known as the *butterfly effect.* For instance, how would have Europe looked today if Archduke Franz Ferdinand of Austria did not visit Sarajevo on June 28 1914 or if young soldier Adolf Hitler had been left blind in 1918?

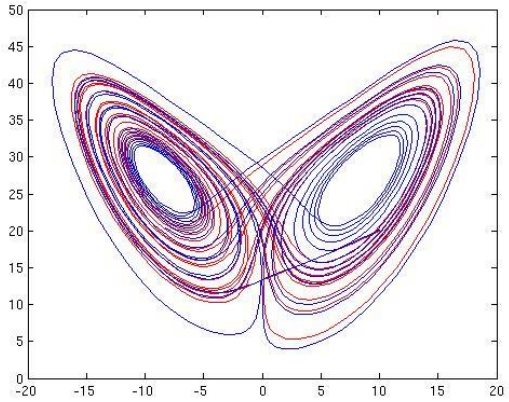


Figure no. 1. The 'Butterfly Effect'

The red and the blue graphs describe two different trajectories of the same complex system starting from two extremely similar sets of initial conditions.

One can observe in the figure that despite the two trajectories are different they have a similar structure – the notion of *attractor.* A complex system orbits around an attractor, never in the same manner, despite a pattern is observable, resulting in unforeseeable movements of the system[2]. Also, according to James Gleick, attractors can be described as forces driving the system's activity towards a common axis.

The notion of attractor also connects chaos theory and fractal geometry – a new way of observing natural world, as it contains unsuspected, but easily recognised patterns[3].

Scholars postulate that fractals should not be defined as a definition could eliminate some interesting cases, but described as *shapes,* not necessarily only 3-dimensional, that are self-similar – it replicates itself at any level – and that have an infinite potential – they are generated by a small number of mathematical equations, from little information[4].

Listing the previously described and explained characteristics and attributes, we reach the conclusion that complex adaptive systems are best encompassed by the next figure: agents are self-organised and they co-evolve as the system exchanges information with the surrounding environment and receives feedback which designs its future transformation.

[2] Sandra, L. BLOOM, *Chaos, Complexity, Self-Organization and Us,* Community Works, America Psychoterapy Review 2(8), August 2000

[3] Michael, FRAME, Benoit B., MANDELBROT, Nial, NEGER, *Fractal Geometry,* Yale University, March 2015, available at http://classes.yale.edu/fractals/, accessed at 25.03.2015

[4] Anirvan, SENGUPTA, *Towards a Theory of Chaos,* International Journal of Bifurcation and Chaos, vol.13, no. 11, pp. 31-49

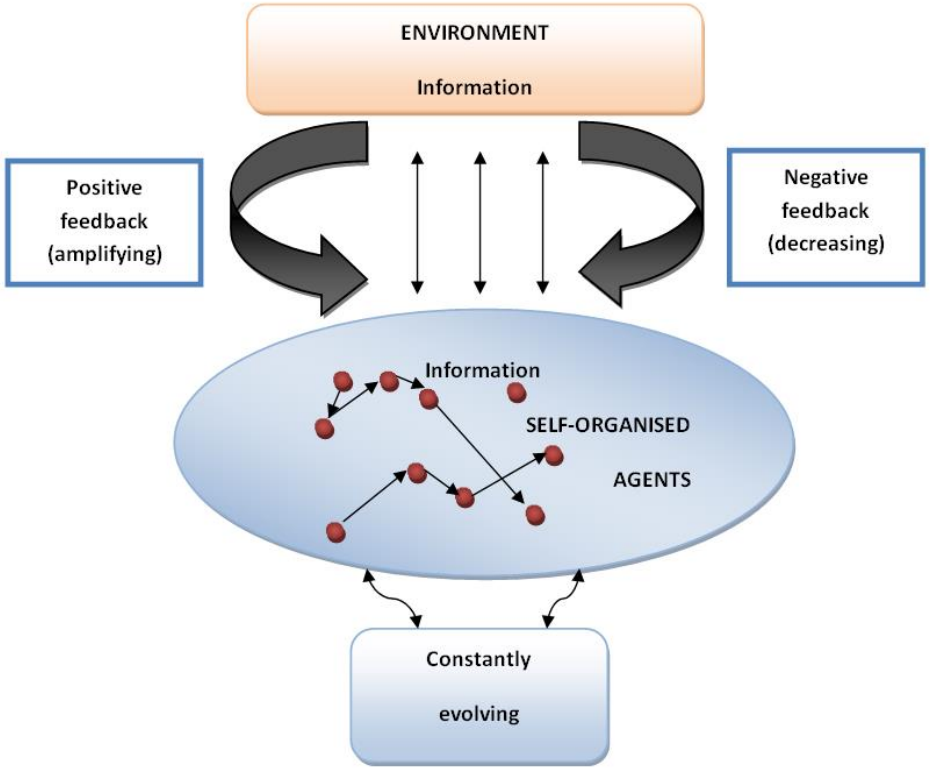


Figure no. 2. Complex Adaptive System

2. Intelligence and CAS Theory

Ours is the age best described by uncertainty, emergence and doubts and the emergence of CAS theory on the security scene should come as no surprise given the fact that intelligence and policy-making communities are in a constant search for panaceas.

Furthermore, in the aftermath of the Soviet Union's dissolution, there is no such thing as a closed national system, resulting in constant information changes between all nation states.

It is beyond the shadow of any doubt that Complexity theory is compelling in this regard as it is based on the study of complex phenomena and hypothesizes that they are until a certain point driven by patterns and understandable. In other words, in the long haul, CAS theory may be seen as the proper base for solving the policy-makers' worst dilemmas.

Intelligence is one of the most, or perhaps the most recent field where complexity theory is applied as it has found popularity in management, economics and markets, ecology and weather forecast.

2.1 Applied CAS attributes

A country's intelligence services and community must be able to dynamically reinvent themselves by progressively gathering information, learning and adapting as the security environment changes. Intelligence decision factors should set a number of objectives that, once reached, help the organization evolve and thus, be more effective in assessing a fast shifting environment.

- Decentralized activity

This is an application of self-organization as it supports the idea that the less the rules, the better the results of the organization, and in consequence, a better security environment.

As an intelligence service possesses the attributes of a complex adaptive system, it is legitimate for all employees – officers and managers – to engage independently in the face of need and changes in the security environment.

Thus, intelligence workers must be able to act more on their own. As ants living in a colony always decide on their own what task to perform and in which manner it should be done, intelligence officers should be granted the right to react – in accordance to legal and organization limits – to developments in the national security. Alongside an application of self-organization, each employee's independence can be seen as a fractal: in proportion to each officer's or managers' experience and expertise, the degree of independence awarded to each employee should include the same criteria, leading to similar forms of decision capacity.

- *Constant search for knowledge*

Intelligence practitioners should be in a constant run for tradecraft and knowledge as they are the main requirements for one's permission to act independently.

Similar to a complex adaptive system's attractor, tradecraft and knowledge should be the very core of each officer's quest.

- *Inclusion and evolution of knowledge workers*

As Peter Druker stated in his 1966 'The Effective Executive' modern society's main factor of production is knowledge. Organizations whose objective is creating, distributing and applying of knowledge, are directly influenced: *knowledge workers*, or analysts in the case of intelligence services, are the ones who dictate the system's productivity and efficiency.

A study conducted at the Bar Ilan University in Israel took the idea of knowledge workers further. According to the research lead by Snunith Shohan and Alon Hasgall, knowledge workers should be seen as fractals as they create the possibility of knowledge management. Due to their responsibility for the integration of their own knowledge, managers may better direct the strategic level operations.

- *Internal information exchange*

The so-called information revolution, brought by the Internet's explosion and the surge in communication, made humankind leave aside the *need-to-know* principle and enter the world of *need-to-share.*

If an intelligence organization wants to evolve, and not only to survive, it has to make use of its best resources: information and people. Practitioners – data collectors, operatives, analysts, tech units and managers – should let aside any competition and share the information they possess.

Hence, gaps filled in the organization's knowledge will not only encourage progress or, in some isolated gases, diminishment, but shall also allow intelligence practitioners *at any hierarchical level* to self-organize and quickly respond to risks and vulnerabilities.

- *Understanding the bigger picture*

Despite daily issues are perceived as the first-hand priority in the intelligence practitioner's current activity, managers should clearly state the long-term, strategic objective.

Given the fact that the security environment is itself a complex system and thus it shifts, employees should know how their work is included in the organization's entire activity in order to better evolve and adapt to outside changes.

- *Constant feedback*

Intelligence services and the entire Intelligence Community must receive more feedback from the national security environment. It is the only manner of learning from and adapting to the changes in the security environment.

The lack of feedback may create a lag in the organization's response to critical issues and it may lead to disastrous consequences.

Conclusions

Hard sciences have dominated research since Isaac Newton discovered gravity. The Newtonian paradigm offered a clean and satisfying depiction of the world and its security. Moreover, the previously stated paradigm, saying that military and intelligence organizations, conflict and war have mechanical tendencies, is no longer to be applied in the current security environment.

Complexity theory and its methaphores embolden us to refer to security in different terms which lead to distinct approaches to the management of intelligence. Also, when applying complexity theory's principles to security, one does expect to find panacea that ensure certainty or exact control, but a manner of understanding uncertainty and apparent disorder.

What this paper is all about is evolution and adaptation, both for organizational survival and security insurance. Nowadays intelligence communities require a Prigoginean manner of thinking: the security, or better said, the insecurity environment is not a fixed given. Complexity, together with self-organization, attractors, fractals etc., used as metaphors are extremely useful for the necessary recruitment, education and training and last, but not least, thinking required for today's intelligence officers.

Despite this, complexity theory does not offer the intelligence community any clear tools such as assigning probabilities to uncertain events. Also, when it comes to decision making, policymakers should not be in search of a universal solution. Instead, they could use a local temporary *best* that allows them to adapt and evolve quickly.

And also, perhaps the main aspect of complexity and chaos metaphors applied to security and intelligence is to warn practitioners not to fall into disorder.

BIBLIOGRAPHY:

1. ALBERTS, David; CZERWINSKI, Thomas J.; *Complexity, Global Politics, and National Security,* National Defense University, Washington D.C., 1997;
2. ANDRUS, Calvin; *Toward a Complex Adaptive Intelligence Community. The Wiki and the Blog;* Central Intelligence Agency, Studies in Intelligence, Vo. 49, No. 3, September 2005;
3. BLOOM, Sandra, L.; *Chaos, Complexity, Self-Organization and Us;* Community Works, America Psychoterapy Review 2(8), August 2000;
4. CHAN, Serena; *Complex Adaptive Systems;* Research Seminar in Engineering Systems, Massachusetts Institute of Technology, 2001;
5. DRUCKER, Peter, *The Effective Executive,* HarperCollins, 1967;
6. FRAME, Michael; MANDELBROT, Benoit B.; NEGER, Nial; *Fractal Geometry,* Yale University, available at http://classes.yale.du/fractals/; accessed at 25.03.2015;
7. HANOVAR, Vasant, *Complex Adaptive Systems Group,* Iowa State University, available at http://www.cs.iastate.edu/~honavar/alife.isu.html, accessed at 23.03.2015;
8. PAVLOS, Antoniou; PITSILLIDES, Andreas; *Understanding Complex Systems: A Communication Networks Perspective,* Nicosia, Computer Science Department, University of Cyprus, 2007;
9. SENGUPTA, Anirvan; *Towards a Theory of Chaos,* International Journal of Bifurcation and Chaos, vol.13, no.11, pp.31-49, 2004;

10. SHOHAM, Snunith; HASGALL, Anon; *Knowledge Workers as Fractals in a Complex Adaptive Organization;* Knowledge and Process Management, volume 12, number 3, pp. 225-236, 2005;
11. TAYLOR, Robert L.V.; *Attractors: Non Strange to Chaotic;* Society for Industrial and Applied Mathematics, SIAM Undergrad Research Online, volume 4, 2010 available at https://www.siam.org/students/siuro/vol4/S01079.pdf, accessed at 20.03.2015.

COMMON ISSUES RELATED TO THE ELABORATION OF DOCTRINAL PRINCIPLES IN THE FIELD OF PUBLIC ORDER AND NATIONAL SECURITY

Antonela-Alina SOFINEȚI
Police officer within the Directorate General for Anti-corruption, Ph.D student within "Alexandru Ioan Cuza" Police Academy, e-mail: antonnella77@yahoo.com

Abstract: *The article tackles the main aspects related to the essential values, the fundamental pillars, professional conduct, ethical standards and basic principles, as well as the traditional guidelines often encountered within the process of elaborating the doctrine associated to the fundamental domain of Public Order and National Security. The author also emphasizes the importance of doctrinal issues related to the complexity of modeling the strategies in this field of research. Also, the article is the segment of a larger project developed within the project POSDRU/159/1.5/S/141086, financed by Romanian Academy.*

Keywords: *values, principles, doctrine, strategy, public order and national security system.*

Introduction

Starting from the definition given by the Romanian dictionary to the "doctrine - assembly of principles of a political system, scientific, religious etc. or set of principles, fundamental ideas of a system", by analogy, we can say that the doctrine of public order and national security summarizes all the principles governing this area, reflecting sound doctrinal values, courses of action, vision and mission of the reference system.

The importance of the doctrine lyes in that it determines and adecvates behaviors, attitudes, actions, aiming to shape or form the thinking or mentality of those to whom it adresses; the doctrine communicate knowledge that transforms or only shapes what is necessary. Where a sound doctrine is missing, the system appears mutilated, inconsistent and the doctrine's beneficiaries only simple dilettantes. The benefits of applying a sound, refreshing and dynamic doctrine are: common approach and understanding, consistency and stability, efficiency and effectiveness.

Following a thorough analisys of the programmatic documents that regulate and govern the public order and national safety area, a series of common elements that stand as fundamental principles can be highlighted within this segment.

The main documents of public policies envisaged for the extraction of the doctrinal elements associated to the public order and security area were the national strategies[1] which

[1] Decision no. 30/2008 on the approval of the National Defense Strategy, published in the Official Gazette no. 799 / 28.11.2008; Government Decision no. 1040/2010 on the approval of the National Strategy for Public Order 2010-2013, published in the Official Gazette no. 721/28.10.2010; Government Decision no. 784/2013 on the approval of the National Countering Drugs Strategy 2013-2020, published in the Official Gazette no. 702 bis/15.11.2013; Decision no. 498/2011 on the approval of the National Immigration Strategy 2011-2014, published in the Official Gazette no. 391/03.06.2011; Government Decision 1156/2012 on the approval of the National Strategy for preventing and combating domestic violence for the period 2013-2017, published in the Official Gazette no. 819/06.12.2012; Decision no. 215/2012 on the approval of the National Anticorruption Strategy 2012-2015, published in the Official Gazette no. 202/27.03.2012; Decision no. 1.142 / 2012 on the approval of the National Strategy against Trafficking in Persons for 2012-2016, published in the Official Gazette no. 820/12.06.2012; Government Decision no. 271/2013 on the approval of the National Cyber Security Strategy, published in the Official Gazette no. 296/23.05.2015; Government Decision no. 775/2005 on the

define and are circumscribed to the area of reference: the security strategy, the defense strategy, the strategy for public order, the strategy against trafficking in human beings, the countering-drug strategy, the strategy for the prevention and fighting against domestic violence, the strategy on immigration, the cyber security strategy and the anti-corruption strategy. These programmatic documents are guided by common elements of doctrine which ensure the applicability, convergence and consistency of the actions and measures enforced in view to the maintenance of public order and safety at national level.

Also, these documents emphasize common guidelines that can stand as a basis for the day-to-day work and can provide the coordinates for an efficient and sustainable public order and national security system. These common principles are: legality, transparency, respect for human rights, priority of the public interest, prevention, availability, dialog and partnership, operational independency, anticipatory and active principle, functional principle, pragmatism, multi-tasking principle, balance principle, principle of continuity, of specificity, subsidiary principle and international correlation principle.

Notwithstanding, these fundamental principles together with the core values, the basic pillars, the elements relating to professional conduct and ethical standards, stand as a foundation in the process of elaborating the doctrine associated to the fundamental domain of public order and national security.

1. Core values and basic issues

The public order forces exercise a noble profession which demands specialized knowledge and skills, as well as high standards of ethics and morality. Hence, all public order forces must adhere to and internalize the enduring *core values* of respect for authority, service for people and responsibility.

The law enforcement forces have respect for authority. Also, they set good examples of decency and morality with regard to the authority. They respect and uphold the laws and the provisions of the Constitution[2] according to which Romania is ”a state governed by the rule of law, democratic and social, in which human dignity, citizens' rights and freedoms, free development of human personality, justice and political pluralism represent supreme values”, and recognize the legitimacy and authority of the leadership. In addition, they believe their commitment into the service of the citizens is above any personal interest.

At the same time, the public order forces must substantiate their existence on the following *pillars*: image, career management, leadership management and equal access to services for all citizens.

The image of the law enforcement agencies within the public order system, once damaged, can affect the morale of the members, as well as the sense of pride within the organization. In this regard, the defamatory accusations of some opinion leaders appeared on the public scene at a certain moment of time, the denigrating judicial cases, aggressively publicized without respecting the universally valid principle of presumption of innocence until a final judgment of conviction, as well as publicly interpreted behavior as inappropriate and without legal foundation by the deciding factors within the field of reference, may constitute examples which can lead to the demoralization of the public order forces and the decrease of their authority and public confidence. Thus, all public order forces act in a manner that would reflect best on them and live by the core values.

A proper implementation of the career management will greatly enhance the personnel profesionalisation process with regards to the procurement, training, promotion, assignment,

---

approval of the Regulation on the procedures for the elaboration, monitoring and evaluation of public policies at the central level, published in the Official Gazette no. 1163/22.12.2005;

[2] Romanian Constitution of 21 November 1991, republished in the Official Gazette no. 767/31.10.2003, art. 1;

placement, awards and retirement of the personnel. One law enforcement agency must formulate a stringent policy and strictly implement the human resources development system, compatible to the equitable distribution of procurement, fair promotion and rationalized approach in assignment, skill development, immediate reward and decent living upon retirement.

In terms of leadership management, the effectiveness of the law enforcement process is reflective of the managerial capabilities and competent leadership of the men and women who run the organization. Therefore, these attributes must be of first criterion in the selection of personnel for employment and deployment purposes.

Also, there must be judicious and equitable distribution of opportunity to prove one's worth in the public order service. The problem on inequity, favored assignment, inequitable opportunity of training, unfair granting of promotion and untimely awarding of achievements, can create an atmosphere of demoralization. The result is inefficiency and lack of teamwork to the detriment of the public order organization. Therefore, the leadership of the organization should address the situation and implement a policy of adherence to the rule on merit system.

In addition, in consonance with the requirements of honor and integrity, all public order forces must have the moral courage to sacrifice self-interest on behalf of the community. Without this moral courage, specific to every structure within the public order and safety system, we would no longer have skilled workers and willing to face the extraordinary challenges generated by the daily rhythm. The sacrifice that differentiates the usual citizen by the specialized worker consists in personal readiness of the latter to commit unconditionally to the serving of citizens in any situation, availability dictated by internal rules of high devotion and altruism. As for setting example, all members of the national public order and security system must set good example in terms of ethics and morality.

2. Professional conduct, ethical standards, customs and traditions

In terms of *professional conduct*, when talking about standards of professionalism, the public order forces perform their duties with integrity, intelligence and competence, specialized skills and technical knowledge, excellence and expertise.

Firstly, *professionalism* means a thorough training of all staff categories working within the national public order and safety system. Secondly, in order to have a flexible and dynamic system, the system should specialize and diversify its methods and means of action so as to reflect an institutional flexibility, a successful and proactive management and especially a decision-making process based on analysis.

The *commitment to democracy* should be a lifestyle. The public order forces commit themselves to the democratic life and values and maintain the principle of public accountability. They at all times uphold the Constitution and are loyal to the country, people and institution. In addition, by raising the social awareness policy, the public order forces are encouraged to actively get involved in social and civic activities, in order to enhance the image of the Romanian law enforcement agencies.

In terms of *physical fitness and health*, all public order forces permanently strive to be physically and mentally fit and in good health. Towards this end, they undergo regular physical exercises and medical examinations and actively participate in different programs of physical fitness or sports development.

From the point of *a secrecy discipline*, public order and security forces guard the confidentiality of classified information against unauthorized disclosure, including confidential aspects of official business, special orders, and communications and other documents, contents of criminal records, identities of different persons and other classified information or intelligence material.

Professional independency refers to the fact that the forces within the public order and safety system seek self-improvement through career development and not solicit influence or recommendation from politicians, high ranking government officials or other prominent citizens. Moreover, they advise their immediate relatives not to interfere in the police service particularly in the assignment and reassignment of personnel.

As for the *public property protection*, all public order forces promote and maintain a sense of responsibility in the protection, proper care, judicious disposition and use of public property which is for their official use or entrusted to their care and custody. In accordance with the command responsibility, immediate chiefs, but also every individual, are responsible for the effective supervision, control and direction of their personnel and see to it that all government resources are managed, expended or utilized in accordance with laws and regulations and against illegal or improper disposition.

When it comes about *ethical standards*, these refer to generally established and accepted moral values. Ethical acts to be observed are the following: patriotism, morality, integrity, devotion, loyalty.

In terms of *patriotism*, the public order and national security forces are traditionally patriotic by nature. They manifest their love of country with a pledge of allegiance to the flag or a vow to defend the national constitution and the legal regulations.

They all adhere to high standards of *morality and decency* and set good examples for others to follow. These rules of morality and decency have their roots in the professional obligations generated by the laws on organization and functioning of the public order system, laws which foresee as a sine qua non condition the adoption of a conduct based on integrity, honor, and respect for the citizens and for the state. In addition, the call for morality and decency must be a personal attribute of those who understand to tie their destiny to such a purpose, namely to be a protector of the society and not only have in mind the material part conferred by their special status. When the professional obligations of the public order forces naturally intertwine with their internal convictions related to the compliance with the law, the result can not be other than giving rise to an attitude of respect for the other citizens.

During their terms of office, they shouldn't be involved in any illegal activities or devoted to vices, nor should they tolerate illegal activities in their respective areas of responsibilities. In this respect, they admit the fact that the test of law enforcement integrity is the presence of personal moral responsibility exemplified by virtuous behavior and non compromising law enforcement personnel.

In terms of *integrity*, the public order forces don't allow themselves to be victims of corruption and dishonest practices. Professional integrity means responsibility in public money spending, as well as unfolding of all security activities in accordance with the rules laid down in different codes of ethics and professional conduct. Also, the law enforcement representatives are obliged to declare any personal interests that may come into contradiction with the exercise of their duties. They are also obliged to take all necessary measures in order to avoid any conflicts of interest or incompatibilities.

Also, the *devotion towards* the job is of the essence. The public order forces must exercise the powers of their service thoroughly, with efficiency, enthusiasm and determination, as well as manifest concern for public goods and refrain from engaging in any activities that are in conflict with their status. Their loyalty is the attachment to the law enforcement authorities, as well as to the values promoted within the public order and safety system. The sharing of the values promoted in the reference system should be voluntary, on its own initiative, and the respect to the principles of a rule of law state should be unequivocally.

In terms of *customs and traditions,* the public order and safety forces adopt the generally acceptable customs and traditions based on the desirable practices specific to the

system. These all serve to inspire the public order forces as the organization fights to attain its goals and objectives.

The customs define the established usage or social practices carried on by tradition that have obtained the force of law. The traditions include the bodies of beliefs, stories, customs and usages handed down from generation to generation with the effect of an unwritten law. Among customs, we can find discipline, manners, camaraderie and courtesy.

The discipline that characterizes the public order and national security system is manifested by instinctive obedience to lawful orders and spontaneous actions, towards the attainment of organizational objectives guided by moral, ethical and legal norms. Discipline is the milestone to develop a career in the national public order and safety system. In this respect, the forces conduct themselves properly at all times in keeping with the rules and regulations of the system.

Gentlemanliness entails that all public order forces are upright in character, gentle in manners, dignified in appearance and sincere in everything they do.

Camaraderie makes the binding spirit that enhances teamwork and cooperation in the law enforcement institution, extending to the community they serve. Public order and safety personnel manifest a deep commitment and concern for one another, as well as for the community.

The courtesy is a manifestation of consideration and respect for the others. Reflections on courtesy can be the salute rendered to the others or the salute to national color and anthem.

3. Fundamental principles

The concept of principle from the lat. "principium"[3] which means "start", may designate based on to the context in which it is used "foundation, basis, the starting point" or "fundamental thesis" or "a result of the laws governing the objective reality, knowledge or action'.

As a rule, due to their high degree of generalization, principles cannot be proven directly, but can be confirmed by their consequences. The concept of "principle" means a provision of maximum generality, which generalizes the effects of the action of a series of objective laws and regulates the educational act.

The rigid and rigorous application of the *fundamental principles* within the framework of the public order and security system is necessary in order to avoid violation of human rights and to maintain the respect for the public service. Thus, the public order and national security forces have attributes related to the prevention and fight against crime in the broadest sense, but also related to the compliance with legal provisions.

Principle of *legality* is the foundation of the national public order and safety area, according to which all policies relating to public order and national security are established in strict consonance with the fundamental human rights and freedoms, as well as in accordance with the rule of law. Thus, principle of human rights observance ensures the guaranteeing of human rights and fundamental freedoms in order to avoid stigmatization, discrimination, insecurity and social exclusion.

The *priority of the public interest* is another principle to be applied, the protection of national interests and values, as well as the fulfilling of the national security objectives being achieved within security architecture and in the spirit of good governance. The forces of the national system of public order, when performing their duties, must give priority to the community and permanently be in the citizens' service because they are community service providers in the broadest sense. In addition, the public order forces also seek and preserve

[3] Maria-Tereza Pirău, Introduction in pedagogy, Bucharest, Ed. Risoprint, 2005, p. 87.

public favor, not by soliciting public opinion, but by constant demonstration of impartiality in offering prompt individual service and congeniality to all members of the community, without regards to their wealth, friendship, social standing and race.

Another principle, *transparency,* requires both citizens' access to information concerning the public order and national security area, as well as recognition and observance of their rights so that they understand the measures and actions unfolded in the area of public order and safety. In this regard, we consider it appropriate the informing, controlling and participation of citizens in the decision-making process in the field of reference. Law enforcement agencies involved in national security issues must be open to society, within the limits set by legal regulations.

Principle of prevention, in the broadest sense, ensures early identification and timely elimination of any occurrence of facts that would undermine public order. Moreover, the public order forces recognize the need for strict adherence to the law, refrain from usurping the powers and authority of the judiciary and admit that the test of their efficiency is in the absence of crime and disorder, as well as the fact that crime prevention is better than crime countering.

Availability and efficiency involve the intervention of law enforcement forces in any situation where a value protected by law is prejudiced, as well as the support and guidance they need to show at any time. Reception of citizens' messages must be prompt and the response adequate. Speedy operations and effectiveness in service delivery to the benefit of the community should be guiding lines in this field. In addition, the participation of our country in concrete actions for the benefit of the other member states in the European Union is of the essence.

The dialogue is based on a networking with the citizens, on the building of a trusty relationship by means of transparency and communication, in accordance with the principles of tolerance, respect and freedom of expression. Networking between institutions and citizens is one of the main instruments that can help boost the public order and safety system and this way tackle all the security needs of the citizens.

Partnership and cooperation against crime, in the broadest sense, are strictly necessary to achieve a climate of public order and national security. Both citizens and law enforcement agencies, at national and international levels, as well as other public or private organizations, must contribute to the improvement and strengthening of the governance act in this area, in order to enhance interoperability and bring resources together towards a public and individual safety. Only through a joint effort performing results can be achieved in this field. The participatory principle requires an integrated approach of the national public order and safety system, such as institutions-forces-citizens, where they are all partners in terms of community problems solving, including emergency situations. This principle also entails the consultation with the civil society in issues of public order and safety because the civil society is the one that gives legitimacy to the public order and safety policy. Non-governmental organizations and other legal entities can collaborate with the public order institutions in order to prevent and eliminate the risks, threats and vulnerabilities to the national security.

Operational independence comes as a counterweight to the participatory principle, but it does not exclude it. Operational independence means that all tasks and duties of the public order and national safety institutions are achieved in accordance with the legal regulations and appropriate hierarchical level, without unlawful interference of other institutions or agencies. But we must lay emphasis on the fact that the participation of other forces in specific missions is of the essence because issues of public order and national safety must be solved in a holistic approach.

The anticipatory and active principle entails that the challenges to the public order and safety system will be addressed and approached as early as possible and rapidly. The means

of identifying future, potential or inherent risks of the public order and safety system, as well as the development of prevention actions capabilities should be more efficient this way.

The functional principle is closely related to the anticipatory one, so that the resources should be consistent with the objectives and concrete action plans or specific targeted policies must be implemented in order to fulfill a public order and safety climate. For this purpose, the law enforcement agencies must develop a set of powerful capabilities, balanced and flexible, in order to manage the risks, threats and vulnerabilities of the public order and safety system, and must have independent resources and facilities.

Principle of pragmatism requires the adoption and implementation of measures and interventions based on scientific evidence and not on political decisions or interests.

Principle of multidisciplinary generates strengthening of state approaches and interventions by combining different disciplinary perspectives and professional practices applicable in the field.

Principle of continuity highlights strengthening and optimization of the results obtained from the implementation of previous public policies or from an ex-post evaluation.

Principle of specification emphasizes the precise defining and implementation of response policies which must be channeled to specific needs and realities for each area of intervention, as well as for local potential involvement in order to achieve the desired objectives.

Principle of subsidiary means ensuring the decision-making process closer to the citizens and permanent monitoring of the need for undertaking specific actions in order to achieve strategic objectives in light of the available possibilities at national, regional or local level.

Principle of international correlation requires the participation and support Romania provides in order to carry out the tasks undertaken by organizations such as NATO, EU, UN, OSCE and Council of Europe. The multilateral, multidirectional and multi-institutional approach of the risks and vulnerabilities to the public order and safety system is the most appropriate one, so as to ensure a reasonable level of mutual safety, order and stability.

Conclusions

In conclusion, the above principles that transcend the documents underlying the public order and safety area can be summarized in: systemic and comprehensive approach to issues of public order and national security; coordination of the public order and safety policies with the economic and social policies; efforts focused on citizen safety and public security; conclusions resulted from the evaluation of the security environment in compliance with the political options and strategic actions.

Analyzing the set of fundamental principles, along with the core values, the basic issues, the elements of professional conduct and ethical standards, we can easily note that Romania shares similar values to other Member States in EU and NATO: human dignity, citizens' rights and freedoms, legality. The assuming of these fundamental values must be effective and tangible for each law enforcement agency; their vector is the political will by which all the three powers in the state, namely the executive, judicial and legislative should understand the importance of a society characterized by a sense of security and work together in order to accomplish this goal.

In this respect, the *set of guidelines* mentioned above is essential for the public order and security system, with multiple advantages. Firstly, following the implementation of these principles, we emphasize the *increased coordination of the elaboration, implementation and evaluation of programmatic documents in the area of reference*. Secondly, we highlight an *increased predictability impact of the implemented programs, but also an improved quality of*

government policies in this area, by means of an extra institutional coordination and cooperation of all social actors. However, advantages to be mentioned are also the *increased efficiency of strategic documents on public order and national safety*, in terms of concrete results and identified malfunctions that may affect these results, as well as the massive involvement of citizens and civil society in the decision-making process on issues of public order and national safety.

The range of principles outlined above is intended to inform the *policy makers and the government representatives, the civil society or NGOs about the need and usefulness of their practical implication in the doctrinal implementation*, in order to make a more dynamic and efficient public order segment so that the safety of the citizens should be a fulfilled desire.

This set of principles identified in the strategic documents of public order and national security are to be applied and implemented; the aim is to increase accountability of their own actions for the public decision makers and to provide a framework through which the civil society can involve in issues of public order and thus, *increase the transparency of the governing act.* In addition, the practical implementation of these principles leads to increased efficiency and quality of the activities unfolded by the central and local authorities in the field of public order and national safety.

The public order and national security area is one of the most important components in a rule of law state and requires the furnishing of a basic efficient public service for the community, with a view to the ensuring of the citizen safety and security. In order to complete an efficient diagnosis for the public order system so as to provide a climate of national safety, a holistic approach of its specific and tangential elements is necessary. By a coherent foundation, essential elements may be furnished for the decision-makers *in order to elaborate a unique national pattern of approaching various programmatic documents in this area*, with applicability in the social life and with a view to a better channeling for the institutional, legal, intelligence and human resources.

The public order and national security system must correspond to the newest strategic and environmental challenges[4], both at national and international level, and in the current dynamic context, a major and permanent coordinate in the security policy is aimed at reducing the risks, threats and vulnerabilities to the public order and security area, by perfecting the specific institutional mechanisms. In this respect, the results of the application of such a set of doctrinal elements could be reflected into *a positive change into the mentality of the decision-makers within the public order and safety system* with regard to the approach and use of future documents of public policies in this area, in order to reach a better management of the system, as well as to furnish the premises of an increased efficiency.

Acknowledgement:

This paper is made 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

[4] European Security Strategy, Bruxelles, 12 December 2003;

BIBLIOGRAPHY:

1. Decision no. 1.142 / 2012 on the approval of the National Strategy against Trafficking in Persons for 2012-2016, published in the Official Gazette no. 820/12.06.2012;
2. Decision no. 215/2012 on the approval of the National Anticorruption Strategy 2012-2015, published in the Official Gazette no. 202/27.03.2012;
3. Decision no. 30/2008 on the approval of the National Defense Strategy, published in the Official Gazette no. 799 / 28.11.2008;
4. Decision no. 498/2011 on the approval of the National Immigration Strategy 2011-2014, published in the Official Gazette no. 391/03.06.2011;
5. Decision no. 62/2006 regarding the National Security Strategy;
6. European Security Strategy, Bruxelles, 12 December 2003;
7. Government Decision 1156/2012 on the approval of the National Strategy for preventing and combating domestic violence for the period 2013-2017, published in the Official Gazette no. 819/06.12.2012;
8. Government Decision no. 1040/2010 on the approval of the National Strategy for Public Order 2010-2013, published in the Official Gazette no. 721/28.10.2010;
9. Government Decision no. 271/2013 on the approval of the National Cyber Security Strategy, published in the Official Gazette no. 296/23.05.2015;
10. Government Decision no. 775/2005 on the approval of the Regulation on the procedures for the elaboration, monitoring and evaluation of public policies at the central level, published in the Official Gazette no. 1163/22.12.2005;
11. Government Decision no. 784/2013 on the approval of the National Countering Drugs Strategy 2013-2020, published in the Official Gazette no. 702 bis/15.11.2013;
12. Maria-Tereza Pirău, Introduction in pedagogy, Ed. Risoprint, Bucharest, 2005;
13. Romanian Constitution of 21 November 1991, republished in the Official Gazette no. 767/31.10.2003.

IMPORTANCE OF CRITICAL THINKING IN IMPROVING INTELLIGENCE SERVICES' ASSESSMENTS

Giorgiana-Raluca STOICA
PhD student at „Mihai Viteazul" National Intelligence Academy in the field "Intelligence and National Security", Bucharest, Romania, e-mail ralluca.stoica@gmail.com

Maria-Cristina MURARU
PhD student at „Mihai Viteazul" National Intelligence Academy in the field "Intelligence and National Security", e-mail: cristina.muraru@gmail.com

Abstract: *Over the years, research in this field indicated that issues concerning the terrorism events on the international scene were determined by errors in intelligence analysis, due to the inability to anticipate risks, despite the existing signals, or to a failed predictive analysis. We can include in this category the terrorist attacks against the USA, Spain or the Russian Federation, the military operation over Iraq justified by the assumption that nuclear weapons are found at the state level, or the conclusion of the 16 American intelligence agencies about the cessation of Iran's nuclear program in 2007.*

The use of critical thinking in the intelligence analysis aims at avoiding such failure by improving the analysts' method of reasoning, particularly overcoming and correcting errors in the cognitive sphere, as well as by getting measurable results meant to anticipate possible action directions.

Keywords*: intelligence, analysis, error, failure, critical thinking*

Introduction

The 21st century information process in a globalized world implies uncertainty and risks, as well as the need to quickly receive and validate a significant number of data, a situation which assumes intelligence analysts' ability to fit in the new environment, including at the cognitive level.

The questions an analyst asks are not mere a working instrument for delving into the existing evidence but a source generating new data which, assisted by technology, leads to new information that help us prevent "strategic surprises". A good reasoning for a good intelligence analysis differs completely from the usual way people, and even analysts, reason.

The initial assumptions of a situation are usually confirmed, by selectively using the evidence, even if there are clear signals that an alternative hypothesis may actually be the correct one.

Thus, people tend to fall prey to a poor thinking, an issue often met in most failures of the intelligence process.

How can analysts avoid this type of poor thinking? The critical thinking represents the answer to that question. The analysts who use of it improve it with their own analyses by identifying the gaps and making use of reflective thinking.

1. Conceptual Approaches

The critical thinking is a deliberate both meta-cognitive (thinking about thinking) and cognitive (thinking) act whereby a person reflects on the quality of reasoning process

simultaneously with reasoning to a conclusion. The thinker has two equally important goals: finding a solution and improving the reasoning skills[1].

In plainer words, the critical thinking supposes using those cognitive skills or strategies which increase the probability of a desirable outcome. It describes purposeful, reasoned and goal directed thinking – involved in solving problems, formulating inferences, calculating likelihoods and making decisions when the thinker uses specially selected skills that are thoughtful and effective for the particular context and type of thinking task. This mechanism involves also the assessment of thinking process - the reasoning which led to a certain decision or the type of factors taken into consideration. Critical thinking is sometimes called "directed thinking" because it focuses on a desired outcome.

The analysis means approaching information by using logical, analog, systemic and communication analysis methods in order to establish the truth, uncertainty or false, or in order to identify and label gaps, vulnerabilities and risk factors which can be threats.

As a product, it is elaborated by the intelligence analyst as a result of a thinking process in which self-assessment of reasoning plays a predominant role, by using specific techniques and methods to establish the cause-effect relation among the gaps, vulnerabilities, risk factors and threats against national security. Intelligence analysts are involved in the acquisition, evaluation, analysis and dissemination of information specific of the area of national security. Each intelligence analyst builds his/her own version of "reality", depending on their experience, cultural values as well as the specific of information.

2. Critical Thinking Process

To adopt the critical thinking, the person who reasons needs eight elements of thought - purpose, question at issue (problem), information (facts, observations, experiences), interpretation (conclusions, solutions), concepts (theories, axioms, principles, models), assumptions (presuppositions), implications and consequences, point of view (perspective), which raise several clear questions on the matter at issue as well as on the thinking process[2].

The research in the field reveals that people always think with a purpose, a thinking which supposes a point of view and is modeled by conscious and unconscious assumptions. Thinking process involves reaching a conclusion deriving from the need to answer to some questions and settle problems based on the available data. The reasoning leads to decisions and consequences.

There are six stages in the critical thinking process, respectively interpretation, analysis, evaluation, inference, explanation and self-regulation[3].

Interpretation is to comprehend and express the meaning or significance of the situations, data, events, and judgments;

Analysis means to identify, using intended inference, the relationships among statements, questions, concepts;

Evaluation is to assess the credibility of statements and logical relationships between statements and events;

Inference means to identify elements needed to draw reasonable assumptions and conclusions as well as to reveal possible consequences;

---

[1] David T. MORE, *Critical Thinking and Intelligence Analysis*, Washington, National Defense Intelligence College, 2007, p. 8

[2] Richard PAUL, Linda ELDER, *Mini-guide de la Pensee Critique Concepts et instruments*, Foundation for Critical Thinking Press, 2008, pp. 1-17

[3] Peter A. FACIONE, *Critical Thinking: What It Is and Why It Counts*, Academis Press, 1998, article available at http://insightassessment.com/pdf_files/what&why98.pdf, accessed at 18.03.2015

Explanation refers to the ability to present the results of reasoning, revealing the arguments which support them;

Self-regulation targets consciously monitoring one's cognitive activities and the results educed, with a view to validating or correcting, if necessary, the reasoning.

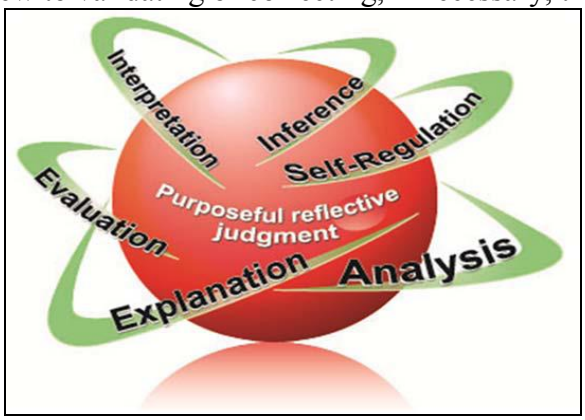


Figure no. 1. Critical Thinking Skills

3. Critical Thinking in Intelligence Analysis

3.1. Optimal framework for formulating pertinent conclusions

The surprises and events difficult to forecast are a constant fact in all nations' history. They are not necessarily caused by the lack of information, but by the nature of the events or cognitive biases. Thus, on the one hand, the general trends are more easily to forecast, comparing with singular events (trend versus phenomena), while, on the other hand, there may be difficult to make the difference between what is true and what is misleading, or to remove predefined ideas of the analyst.

To reduce the risk of unpredictable situations in a constantly-changing world, the intelligence analysts, more than any other category of analysts, have to develop skills of using analytical instruments which make them aware when the old predefined ideas cannot be applied any longer.

In intelligence analysis, the critical thinking provides the intellectual instrument necessary to reflect.

The significant volume of online information corroborated with the high risk of manipulation through open sources, imposes an introspective calculation on treating information and reflecting the way the analysis is reasoned.

The analyst can apply several methods of analyzing, check which one brings the best outcome or compare the outcomes and, if differences, identify they origin.

In drawing conclusions, the analyst has to answer the following questions: "Do my inferences derive from the available data?", "Are my conclusions logical?" The conclusions may often generate new data searching and reveal associated scenarios.

Intelligence analysis process needs an intellectual effort to order the data according to their importance degree and then a relevant conclusion is drawn through an individual assessment assisted by reasoning.

Reasoning supposes three forms – induction, deduction and abduction[4] - seeking to create an objective connection between analyst's beliefs and information that suggest a trend different from the previously identified one.

Inductive reasoning suggests a wide range, a series of potential future results or actions. It is essential in issuing warnings / forecasts, identifying a trend. Thus, based on previous perceptions, the current actions will indicate a possible trend, but not necessarily for it to materialize.

On the other hand, in particular, deductive reasoning supposes identifying the elements necessary for the issuance of assumptions and arrive at a reasonable conclusion and highlighting the possible consequences.

Abductive reasoning represents an alternation between induction and deduction, the aim being to identify assumptions. Thus, if in the case of induction and are given conclusion and minor premise, being necessary to establish the major one, in deduction are given two premises, requiring a conclusion, abduction is the foundation of minor premise when are given the major premise and conclusion[5].

In other words, while inductive reasoning reveals "that something might be true", the deductive reasoning certifies that "something is true". Nevertheless, both forms are limited, running the risk that inductive reasoning generates multiple solutions with similar probability degree, and the deductive reasoning is affected by the analyst's believes. In this situation, the abductive reasoning showing that "something is plausibly true" can compensate the limitations of the other two.

Despite individual limits, the corroboration of the three forms offers the possibility of a thorough examination of information with a view to drawing relevant conclusions. The critical thinking provides this framework by making sure that each reasoning form is adequately used. This method extends to the whole intelligence analysis process.

3.2. Response to Error Issue

Intelligence analysts are constantly faced with incomplete or unclear data, contradictory sources as well as with deliberate attempts to mislead (*denial and deception*) of the authoritarian regimes of some countries that deny access to data of interest (*such as military programs*). The specialty literature refers to the use of misleading techniques by Russia using the term "maskirovka"[6].

In order to improve analysts' reasoning as well as to avoid misleading techniques, it is necessary to change the management of data available to them and establish the analysis method that can produce a solution to the investigated problem. Thus, in selecting and assessing data, the analyst should guide himself/ herself by the following questions: "What is the chance of being misled?", "Why is this happening?", "Why is this source credible?", "If the opposite scenario is indeed true, what data supporting it should I consider?", "What are my predefined ideas?".

The criteria based on which data credibility should be assessed are authenticity, accuracy, and flexibility. However, authenticity is not absolute, but it depends on the time and background, while flexibility can be tested by obtaining the same data from different collection sources.

---

[4] William MILLWARD, *Life in and aut of Hut 3*, in F.H. HINSLEY and Alan STRIPP: *The Codebreakers: The Inside Story of Bletchley Park*, Oxford University Press, 1993, p. 17.

[5] Ioan Bus, *Argumente transcendentale și inferența abductivă, 2003*, p. 45, article available at http://www.roslir.goldenideashome.com/archiv/2003_3-4/12IonBus2003.pdf, accesed at 24.04.2015

[6] David T. MORE, *Critical Thinking and Intelligence Analysis*, Washington, National Defense Intelligence College, 2007, p. 25.

Critical thinking focuses, in fact, on the process on elaborating true and valid conclusions (knowledge creation). The four problems[7] arising from the process of reasoning in intelligence are the following: insufficiency, irrelevancy, indeterminacy and the instrumentality.

Insufficiency derives from the relationship of data to knowledge in the network of analysis. The vast majority of the knowledge developed by analysts will be ultimately based on collected data, but this data is inevitably insufficient in at least two ways: it is limited in its scope and therefore does not cover all the issues that the analyst must consider; it is limited in its reliability, because it consists of only purported facts (namely, those that may prove false). Therefore, the *intelligence* professional has no alternative but to rely on incomplete and often inaccurate data, and he/ she should assume, instead, that much of the relevant data is missing while some of the available data is mistaken or misleading.

Irrelevancy derives from the relationship between information and knowledge in the network of analysis. The knowledge that analyst infers comes from the information to which he/ she have access to, but which contains much more than actually necessary to elaborate products. Most of the information can even prove irrelevant to the question at hand. The practitioner can never assume that the information he/ she has is relevant to the issue he/ she is investigating, but he/ she can assume instead that "most information" is, despite appearances, not relevant.

Indeterminacy derives from the relationship between knowledge and the entire analysis network, and the world itself (the events being analyzed). Most of the events that analyst seeks to understand and especially to anticipate, are not inevitable (not all the information necessary to project them can be acquired). Instead, even if analysts knew everything to be known about a particular terrorist, for instance, it would still not be possible to infer with certainty what that terrorist would do. The decisions and actions of human agents, as well as many natural processes, are indeterministic (they are not the inevitable consequences of prior causal factors, but rather are only one of several different possible outcomes, each having some real possibility of occurring). Only one set of future events will actually occur, but one cannot say it is the only set that had a "real chance" of occurring. The analyst can never assume that things might go in only one possible way, but he/ she can instead assume that a series of different, incompatible "futures" could occur. He/ she has to determine what would occur if each of the different alternatives were to happen.

Instrumentality derives from the relationship between understanding and knowledge. Through analysis, one can acquire knowledge not simply for its own sake, but instead to specifically address the "challenges" faced by consumers, a fact that creates substantial additional constraints on "knowledge-acquisition". At the same time, one can neither establish an adequate period of time to do analysis and nor can assume that the decision-maker is simply an objective observer without policy goals.

Critical thinking can diminish some common causes of failures and provide the means by which they can be avoided in the future. Specifically, any information process based on this type of thinking can compensate for the following failures when:

Analysts are wrong. It is not realistic to expect that analysts are never wrong. Regardless of the processes they use, analysts make mistakes. Anthropologist Rob Johnston defines errors as „factual inaccuracies in analysis resulting from poor or missing data"[8].

---

[7] Noel HENDRICKSON, *Critical Thinking in Intelligence Analysis*, London, International Journal of Intelligence and CounterIntelligence, vol. 21, no.4, 2008, pp. 679-693.

[8] Rob JOHNSTON, *Analytic Culture in the U.S. Intelligence Community*, Washington, Central Intelligence Agency, 2005, p. 6, book available at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-

Similarly, information failures are „systemic organizational surprises resulting from incorrect, missing, discarded, or inadequate hypotheses". Critical thinking reduces such types of error, providing the means to assess reasoning errors when they occur as well as before becoming systemic failures. Such a meta-cognitive approach of the analytical process facilitates monitoring at its highest levels. Studies have revealed that cognitive limitation is the most important source of intelligence failures, which is also most difficult to remedy[9]. According to cognitive psychology, people fail to realize the mental mechanism by which perceptions are formed. Yet, it is an active rather than passive process, in which reality is built, not recorded, based on information provided through the senses. What people perceive is influenced by past experience, education, cultural values and organizational norms. Usually, people tend to perceive what they expect to perceive. Events consistent with expectations are processed easily, while those that contradict them tend to be ignored or distorted in subconscious. Once developed, cognitive biases determine future perceptions of a phenomenon. Thus, new information is assimilated to existing images[10]. Initial interpretation is maintained until the contradiction becomes so obvious that it requires a change of perception. Cognitive biases are therefore defined as mental errors caused by simplified information processing strategies. Mindsets have the following characteristics: they are quick to form and resistant to change; new information is usually made to fit into the existing conceptual framework; an initial impression based on incomplete or ambiguous data is likely to persist even after better information becomes available to the analyst.

Policymakers ignore intelligence. On the one hand, information must be convincing and compel policymakers to pay attention to the content. On the other hand, information should not tell decision makers what to do.

Adversaries deny and deceive. Critical thinking reduces the effects of adversarial denial and deception by leading analysts to consider all possibilities, to question assumptions and biases, to examine systematically the validity of evidence being considered, and to take seriously anomalies in the evidence.

Adversary is more capable. In any adversarial system, there are winners and losers. While analysts can do everything possible to ensure their work is correct, they rarely work with all the evidence, and may still be deceived. In such cases, they may come to wrong conclusions. Critical thinking, however, by providing structure and oversight to their reasoning, provides an audit trail. In this case, the means by which the analytic conclusions were reached can be subsequently reviewed, errors and deceptions revealed, and steps taken to improve the process so that the failure is not repeated**.** Indeed, because of its focus on the process, critical thinking becomes a powerful tool for evaluating and enhancing analytical reasoning[11].

---

publications/books-and-monographs/analytic-culture-in-the-u-s-intelligence-community/analytic_culture_report.pdf, accessed at 24.03.2014

[9] Richard J. HEUER Jr., *Limits of Intelligence Analysis*, Orbis, 2005, pp.75-94, book available at http://www.worldaffairsboard.com/attachments/staff-college/20727d1273228985-ebo-sod-limits-intelligence-analysis-fpri-winter-2005-heurer-.pdf, accessed at 19.03.2015

[10] Magdalena A. DUVENAGE, *Intelligence Analysis in the Knowledge Age. An Analysis of the Challenges facing the Practice of Intelligence Analysis*, Stellenbosch University, 2010, p. 102, article available at http://hdl.handle.net/10019.1/46428, accessed at 24.03.2015

[11] David T. MORE, *Critical Thinking and Intelligence Analysis*, Washington, National Defense Intelligence College, 2007, pp. 79-80.

3.3. Examples of Analytical Failures

Most intelligence analysis failures are caused by misinterpretations, not by collection errors – the available information was ignored or rejected because it did not fit the analyst's mental model.

Relevant in this regard are the conclusions issued prior to the coalition troops' intervention in Iraq in 2003 or those on stopping the Iranian nuclear program in 2008.

In the case of Iraq intervention, a US Senate report revealed „uncertain clues were used as evidence and information that contradicted the overall picture were ignored". Under such circumstances, the intelligence services sought data that met the policymakers' expectations[12]. Thus, the information gap was filled by the analyst's mental model. Even if the U.S. intelligence community had an inside source close to the authorities in Baghdad, it would have still questioned the information obtained, viewing it as part of a deception plan.

The French Centre for Intelligence Studies labeled the 2007 report of the National Intelligence Directorate in which 16 U.S. intelligence agencies claimed that Iran had halted its nuclear program since 2003 as an intelligence error[13], as it was shown that the Iranian state has not taken steps in this regard so far, but on the contrary, it is suspected of still developing nuclear weapons.

One can conclude that analysts' prejudices and mindset as well as their false assumptions have prevented them from realizing Iran's real intentions, as the report conclusions were based on the wiretap tapes in which Iranian authorities were criticizing the halt of the military program. However, American experts did not take into account the risk of manipulation by Iranian authorities.

Also, terrorist attacks recorded worldwide (including those on September 11, 2001 - United States of America, April 11, 2003 - Spain, February 6, August 31, 2004, November 27, 2009 Russian Federation) in recent years could be considered errors of intelligence analysis, by the fact that relevant organizations could not predict the risk of such events.

Both experts and media has advanced the hypothesis that the last events occurred in the terrorism sphere - Boston bombing April 2013 and the one occurred in France at the beginning of this year- has allegedly been facilitated by an intelligence analysis error of the intelligence services from the both countries, which could not forecast the risk[14].

Apparently Tamerlan Tsarnaev, the main Boston bombing suspect, has managed to escape the attention of intelligence services when he left Russia in 2012, his later return to the U.S. being overlooked due to human error.

A similar approach was advanced in France, where the French intelligence services were warmed at the ending of 2014 by the Algerian counterparts of the imminent terrorist attacks. Cherif and Said Kouachi, the two brothers who committed the attack on satirical newspaper office Charlie Hebdo, Amedy Coulibaly , who took hostages people in a store and his girlfriend, Boumeddiene Hayat, all four were connected both between each other, as and an extensive network of extremists in Europe. Moreover the two people responsible the attack on Charlie Hebdo, were in the attention of intelligence services, especially since one of them

---

[12] Richard J. HEUER Jr., *Limits of Intelligence Analysis*, Orbis, 2005, pp. 75-94, book available at http://www.worldaffairsboard.com/attachments/staff-college/20727d1273228985-ebo-sod-limits-intelligence-analysis-fpri-winter-2005-heurer-.pdf, accessed at 19.03.2015

[13] Alain RODIER, *Pourquoi les americains ont plie devant les iraniens*, Centrul Francez de Studii de Intelligence, note no.111, 2007, article available at http://www.cf2r.org/fr/notes-actualite/pourquoi-les-americains-ont-plie-devant-les-iraniens.php, accesed at 17.03.2015

[14] Christopher DICKEY, *The Boston Bombing Intelligence Failure*, 16.04.2013, article available at http://www.thedailybeast.com/articles/2013/04/16/the-boston-bombing-intelligence-failure.html, accessed at 18.03.2015

went to jail 10 years ago on suspicion of links with jihadist environment[15]. However, supervision by the authorities of the two brothers stopped mid-2014, fact that may be categorized as an intelligence failure.

Conclusions

Critical thinking is not perfect, because people thinking critically do make mistakes. But the process of introspection and self-correction through which always passes the one who practice critical thinking makes him commit fewer mistakes than those who don't think critically.

Thus, critical thinking is self-directed, self-disciplined, self-monitored and self-corrective and that requires rigorous standards of excellence and mindful command of their use.

The use of critical thinking leads to improved effective communication ability to solve problems.

Without critical thinking, people would be more easily exploited, being unthinkable, for example, economic or legal system where critical thinking isn't applied because the lack of critical thinking would make impossible to interpret market trends. Using critical thinking by an informed society is a necessary condition for the success of democratic institutions.

Critical thinking is an extremely beneficial in the intelligence work, this cognitive mechanism leading to mitigation of errors inherent to the analytical process generated by predefined ideas, reassessment by the decision-makers of their own perceptions and assessments on specific topics, limitation of the risk of analysts being voluntary misled by opponents, transparent reasoning mechanism so that all reasoning steps are explained and easy to follow and reviewed.

This way, both intelligence officers and information recipients will no longer focus on the analysis result, but on its development process**,** a fact that will generate a more efficient implementation of the expert assessments.

BIBLIOGRAPHY:

1. BUS, Ioan, *Argumente transcendentale şi inferența abductivă, 2003*, p. 45, article available at http://www.roslir.goldenideashome.com/archiv/2003_3-4/12IonBus2003.pdf
2. DICKEY, Christopher, *The Boston Bombing Intelligence Failure*, The Daily Beast, 16.04.2013, article available at http://www.thedailybeast.com/articles/2013/04/16/the-boston-bombing-intelligence-failure.html
3. DUVENAGE, Magdalena, A., *Intelligence Analysis in the Knowledge Age. An Analysis of the Challenges facing the Practice of Intelligence Analysis*, Stellenbosch University, 2010, article available at http://hdl.handle.net/10019.1/46428
4. FACIONE, Peter, A., *Critical Thinking: What It Is and Why It Counts*, Academis Press, 1998, article available at http://insightassessment.com/pdf_files/what&why98.pdf

[15] Shashank JOSHI, *Charlie Hebdo attack: A French intelligence failure?*, 10.01.2015, article available at http://www.bbc.com/news/world-europe-30760656, accessed at 26.03.2015

5. HENDRICKSON, Noel, *Critical Thinking in Intelligence Analysis*, International Journal of Intelligence and CounterIntelligence, vol. 21, no.4, London, 2008
6. HEUER, Richard J., Jr., *Limits of Intelligence Analysis*, Orbis, 2005, available at http://www.worldaffairsboard.com/attachments/staff-college/20727d1273228985-ebo-sod-limits-intelligence-analysis-fpri-winter-2005-heurer-.pdf
7. JOHNSTON, Rob *Analytic Culture in the U.S. Intelligence Community*, Central Intelligence Agency, Washington, 2005, p. 6, book available at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/analytic-culture-in-the-u-s-intelligence-community/analytic_culture_report.pdf
8. JOSHI, Shashank, *Charlie Hebdo attack: A French intelligence failure?,* 10.01.2015, article available at http://www.bbc.com/news/world-europe-30760656
9. MILLWARD, William, *Life in and aut of Hut 3*, in HINSLEY**,** F.H.; STRIPP, Alain: *The Codebrakers: The Inside Story of Bletchley Park*, Oxford University Press, 1993
10. MORE, David T., *Critical Thinking and Intelligence Analysis*, National Defense Intelligence College, Wasghington, 2007
11. PAUL, Richard; ELDER, Linda, *Mini-guide de la Pensee Critique Concepts et instruments*, Foundation for Critical Thinking Press, 2008
12. RODIER, Alain, *Pourquoi les americains ont plie devant les iraniens,* French Center of Intelligence Studies, note no.111, 2007, article available at http://www.cf2r.org/fr/notes-actualite/pourquoi-les-americains-ont-plie-devant-les-iraniens.php

DE LEGE FERENDA CONCERNING THE ENTRANCE, STATIONING, DEPLOYING OF OPERATIONS OR TRANSIT OF FOREIGN ARMED FORCES ON ROMANIAN TERRITORY

Florin MACIU
Brigadier General, PhD, legal adviser, Ministry of National Defence
fmaciu@yahoo.com

Abstract: *Lately, an extremely serious and very complex situation has been created, with possible grave consequences regarding the security of the Black Sea region, but also related to the Euro-Atlantic area, with elements that mark the periods of time before the beginning of a military unhidden armed conflict, of a great amplitude. These elements are: annexation of foreign territories, rebel support from a foreign state, thousands of civilian and military victims, committing abominable deeds like shooting down a civilian plane, without any connection with the, conflict significant decrease of diplomatic channels or using, a dialogue of the deaf mutual accusations and threats, taking countermeasures and counter-countermeasures, violation of international agreements, escalation of the number of military exercises in the close vicinity of the assumed opponent, forcing coercive economic measures, founding new military bases inside the conflict zone.*

In order to secure the defense capacity of the country, through the permanent presence of allied forces on Romanian territory, we should take the necessary measures in order not to stumble ourselves in our own law thicket. This means amending the current legislation to soften the path of implementing the intentions of receiving in our country military forces belonging to allied states. These should have not only an intimidating part towards any aggressors, but also a part of an active participant in defending against invasion. Legislative measures should be adopted in a timely manner, in order to optimize rules regarding the stationing of foreign armed forces on the country's territory. Some of the law texts, susceptible of castigation, as well as some recommendations are presented in this work. The others refer to the exploitation of some international juridical instruments.

Keywords: *security, annexation, alliance, regulation, modification, completion, amendment, foreign military presence, Romanian territory, fiscal facilities, support*

Introduction

For more than a year, the Romanians have been overwhelmed with extremely grave news, regarding dramatic events concerning the aggression upon Ukraine, meaning actions that without any exaggeration, can lead to a new world conflagration. The Black-Sea region security has always been a trouble spot, marked by several complications of the situation in the area, as well as complex elements which interact, creating instability. However, currently, more serious than in the past, we acknowledge the exacerbated violence and turmoil reaches paroxysm.

One by one, overcoming our imagination, significant things happen, meant to cause not only panic, but also changes in the administrative geography or memorable scenes in the contemporaneous history. The entire Euro-Atlantic area winces when witnessing the annexation of some foreign territories, the impertinent support offered to the rebels from another country, the numerous violence acts ended with thousands of civil and military victims. We are horrified because of the intensification of abominable deeds, culminating with the shooting down of a civilian airplane, belonging to a state which is not involved in the conflict and whose passengers were completely innocent. The diplomatic channels between

the opponents diminish consistently and when they still exist, they are being used for a dialogue of the deaf, full of accusations and mutual threats.

International agreements are ignored or biased explained, countermeasures and counter- countermeasures are taken, economic coercive measures are enforced and the price for energy is used as a genuine and efficient weapon in the confrontation, the number of military exercises that should intimidate through the force parade is escalated and almost all are taking place in the near proximity of the opponent. In this context, we reach the situation when the states from the vicinity of the conflict area wish to increase their own security, to perpetuate the presence of some allied foreign military armed forces, on their territory and they even compete in offering the necessary infrastructure for establishing the so called foreign military bases.

In this situation, it is obvious that Romania being located on the East flank of the North-Atlantic Alliance and having Ukraine as neighbour, is as well, concerned with the consolidation of the factors that help for self defense. In another opinion presented in a work, meant to be published later, we showed that it is saner, giving the current situation, for all allies to have a pragmatic position, meaning we should strongly orientate towards creating and maintaining a solid defense capacity, including establishing permanent foreign military entities on the countries territory, instead of making theoretical assumptions concerning the identification of the side which committed a violation of the international agreement between NATO and the Russian Federation, signed in Paris 1997[1]. In our opinion, Romania's greatest goal is preserving the national state, independence and maximizing the functionality of the real democracy principles, goals that can't be achieved under foreign occupation, a nightmare which, unfortunately, in our opinion, can become reality.

[1] As she was in an official visit in Riga, Letonia, the German chancellor, Angela Merkel rejected some local politicians and intellectuals' requests to establish a permanent military force from West in the region, although she warranted to support the Baltic countries against a possible Russian threat („*Merkel Promises Support for Baltic States Alarmed by Russia*", Juris Kaža, August 18, 2014, The Wall Street Journal, World News, http://www.wsj.com/articles/merkel-promises-support-for-baltic-states-alarmed-by-russia-1408383489, accessed on the 12 of March 2015). The reason the chancellor offered for the refuse was that by installing a permanent military presence East from the Alliance is that it violates the agreement between NATO and Russia.
The Latvians request was caused, naturally, because of the annexation of Crimea Peninsula to Russia, which alarmed the former stated from the ex-soviet space but also the NATO state members East from the Alliance. Trying to explain her position, implying the agreement for increased preparations for deploying troops in the area without agreeing with the permanent NATO presence, the chancellor underlined that based on the International Cooperation Treaty from 1997 between NATO and the Russian Federation, both sides agreed not to treat each other as opponents and has reminded that a permanent NATO presence in the area would violate the agreement.
At the beginning of June 2014, the defense ministers from the NATO member states have agreed to answer to the Ukraine crisis with the amplification of the protection measures in Eastern Europe („*NATO Agrees To 'Readiness Action Plan' To Counter Russia*", By AGENCE FRANCE-PRESSE, June 03, 2014, Defense News, http://archive.defensenews.com/article/20140603/DEFREG01/306030034/NATO-Agrees-Readiness-Action-Plan-Counter-Russia, accessed on the 12 of March 2015), but have stated that they will act in the limits set by the Moscow Treaty after de Cold War. Russia's Ambassador at NATO, Alexander Grush, stated a day earlier that the temporary troops and airplane deployment belonging to the Alliance over the number existing in the NATO member states, like Poland and the Baltic countries, equals with a violation of the treaty. The Russian charges, as we said earlier, have had some echoes through the allies, meaning some have said that the treaty clearly forbids the deploying of troops and combat means for creating new permanent presences in Eastern Europe.

1. De facto situation

Both USA and the European Union consequently reaffirm that they strongly disagree with the Russian activities in Ukraine. One year later from the controversial referendum organized in Crimea, Jennifer Psaki, the spokesman for the American State Department, stated in the middle of March 2015, almost simultaneously with Federica Mogherini's intervention, the chief of European diplomacy, that these state structures militate against the illegal annexation of the peninsula by Russia. Dimitri Peskov, the spokesman of the Russian President, Vladimir Putin, answered shortly announcing that Crimea's territory is part of Russia and this matter shall not be discussed with anyone[2].

In convergence with the position of the European Union states and North America, Ioan Mircea Paşcu presents to the Subcommittee for security and defense of the European Parliament a report draft that approaches, from a military strategic point of view, the situation from the Black Sea region, after Crimea's annexation. According to him the military strategic situation from the Black Sea has changed dramatically. The Russian force becomes a striking military group, with high offensive potential, including disembarkment[3]. In this context, some elements are not to be neglected, such as an escalation of the conflict by using nuclear armament, an aggravation of the situation of the minorities or dangerous economic implications for the Union.

1.1 .Scenarios

Also, Mircea Paşcu, in the above mentioned document, presents briefly, the possible escalation of the situation, according to which Russia might approach Romania's boarders through annexations and occupations of Ukrainian territories. We specify that it is not about predictions, but about theoretical possibilities, with chances of becoming real.

A. Russia occupies in the Black Sea zone a 50 km corridor that connects the recognized Federation territory, the territories that were occupied by rebels and Crimea peninsula.

Upon this script, there is also option A+, in which Russia will reach Odessa. This option was built by the Stratfor[4] analysts and it was also presented by the former foreign affairs minister, Cristian Diaconesco, beside the historian, Armand Gosu[5]. In this situation the Russian movement towards Galaţi would take two hours, a Russian airplane would reach Bucharest in several minutes, as well as a missile. The continental Romanian plateau, a future great energy source would also be exposed, simultaneously with a possible energetic independence of our country.

B. Russia takes over the South of Ukraine and reaches Transnistria, building a connection bridge between the territories with Russian population from the South of Ukraine.

---

[2] *"Moscow celebrates a year since the annexation of Crimea through a concert-meeting in the Red Square where Vladimir Putin is expected"*, Flori Tiulea, Agerpres, 18th of March 2015, http://www.agerpres.ro/externe/2015/03/18/moscova-sarbatoreste-un-an-de-la-anexarea-crimeii-printr-un-miting-concert-in-piata-rosie-la-care-este-asteptat-si-vladimir-putin-11-34-24, accessed of the 18th of March 2015;

[3] *"Ioan Mircea Paşcu: The military equilibrium from the Black Sea region changed in Russia's favour"*, Ionuţ Mares, Agerpres, 17th of March 2015, http://www.agerpres.ro/externe/2015/03/17/ioan-mircea-pascu-echilibrul-militar-din-regiunea-marii-negre-s-a-schimbat-in-favoarea-rusiei-12-22-03, accessed on the 18th of March 2015;

[4] *"Stratfor analyzes Romania's chances in from of Russian invasion"*, e-politic.ro, 11th of March 2015, http://e-politic.ziuanews.ro/dezvaluiri-investigatii/stratfor-analizeaza-ce-sanse-ar-avea-romania-in-fata-unei-invazii-rusesti-168420, accessed of the 12 of March 2015;

[5] *"The worse situation crossed by Romania in the last decades. A diplomat and historian, relating about the danger of a war with Russia"*, Pro TV, 22nd of February 2015, http://stirileprotv.ro/emisiuni/dupa-20-de-ani/e-lucrul-cel-mai-grav-trait-de-romania-in-ultimele-decenii-un-diplomat-si-un-istoric-despre-pericolul-razboiului-cu-rusia.html, accessed of the 12 of March 2015;

This scenario was thought by the people in Stratfor and it would last 3-4 weeks until reaching the finality and the veracity is confirmed also by the former affairs minister of Germany, Joschka Fischer. Apparently, for the Russians this plan would be more expensive, a large number of military would be needed. Russia's succes wouldn't be impossible.

C. Russia launches a conventional attack over an East-European NATO member state, aiming for the neutralization of Ukraine and discussing about the Alliances response capacity, namely checking the functionality of article 5 provisions from the NATO Treaty.

The veracity of this theory is confirmed by sir Adrian Bradshaw, the Deputy commander of the NATO forces in Europe, who underlines the risk of nuclear confrontation, in such a case. Retired general Degeratu Constantin, former Chief of General Staff, confirms the accuracy of this scenario and, furthermore, identifies possible victim states: Estonia or Romania[6].

As we can conclude, the scenarios that follow from Russia's intervention in Ukraine have a common factor, a very close and dark future for Romania.

1.2 Romania's neighbours attitude

Let's concisely revise the position of the states who are in the vicinity of Romania, so that we can establish the foreign elements on which our country can rely in order to quickly strengthen the defense, in case one of the horror scripts, mentioned above, comes true.

Moldavia, a state that we consider brotherly, which aspires to the European Union, but which actually depends, from the energy point of view, on the Russians, has the 14th Army on its territory, is part of a latent conflict with separatist Transnistrians. We think that many of the Moldavian citizens are Russian speaking and they have quasi-communist ideas, very unfriendly for Romania.

Ukraine was divided by the Russians, partly occupied by them, having huge external debts being situated on the edge of bankruptcy.

Hungary, which seams concerned with its personal interests, sometimes deviating, maintains good relationships with Russia, ignoring the warnings coming from the European Union, not being very good neighbour to Romania, sometimes obviously showing its hostility through different characters who are very popular in this country. The former model we followed before entering NATO lost its glow and stands out in a negative way in what concerns democracy.

Serbia is a good partner of the Russians by tradition, as well as Bulgaria, which, even if it's a member of NATO, can become anytime an outpost of the Russian Federation[7].

From all these states, Romania pays to Gazprom the highest price for Russian gas, which shows that the neighbours have assured the Russian good will, through a duplicating behaviour.

1.3 Romania's defense policy

Recent information underlines new elements regarding the Russian Federation military activity in Crimea region. Here, they will bring strategic Tu-22M3 airplanes, capable to transport nuclear missiles[8]. Ukraine's president, Petro Poroşenko, mentioned these days about

---

[6] *"If Romania was attacked by Russia"*, QMagazine, 10th of March 2015, http://qmagazine.ro/ce-nu-se-vede-la-tv/daca-romania-ar-fi-atacata-de-rusia/, accessed of the 12 of March 2015;

[7] *"Impetus Putin. The opportunity for a tandem between Romania and Poland"*, Laurenţiu Mihu, România Liberă, 11th of March 2015, http://www.romanialibera.ro/politica/institutii/stimulentul-putin--oportunitatea-unui-tandem-romania-polonia-370623, accessed of the 12 of March 2015;

[8] *"Russia is replaying the intimidation card. It moves the nuclear weapons closer to Europe"*, Oleg Cojocaru, Rusia.ro page, 17th of March 2015, http://www.paginaderusia.ro/rusia-iar-joaca-cartea-intimidarii-muta-armele-nucleare-mai-aproape-de-europa/, accessed of the 19th of March 2015;

a risk of a great conflict, in the Black Sea region[9]. This concerning news shows the rightfulness of the measures taken in the beginning of February, at the NATO defense minister's reunion in Brussels.

It has been decided that Multinational Command and Control Divisions should be established, for integrating NATO forces on the territories from the East border of the Organization. Romania agreed with this proposal and engaged to do everything in its power regarding this matter. Furthermore, Romania agreed to host on its territory a Multifunctional Headquarter Division, operational on 2016.

From the foreign affairs minister, Bogdan Auresco to Klaus Johannis, Romania's president, including Mircea Duşa, the minister of national defense, people with great reasonability have agreed with these measures and the Army has begun to prepare the relevant documents and to take all necessary actions with the highest professionalism.

2 *De lege ferenda* concerning the entrance, the stationing, the deploying of operations or the transit of foreign armed forces on Romanian territory. Conclusions.

For strengthening the country defense capacity through the permanent presence of the allied forces on Romania's territory, we should take the necessary measures in order not to stumble ourselves in our own law thicket. This means amending the current legislation to facilitate the receiving in our country of military forces belonging to allied states. These should have not only a deterrence part towards any aggressors, but also a part of an active participant in defending against any threatening invasion. Legislative measures should be adopted in a timely manner, in order to optimize rules regarding the stationing of foreign armed forces on our country's territory. Some of the law texts, which are susceptible of castigation, as well as some recommendations are presented in this paper. The others refer to the application of some international juridical instruments.

2.2 Abrogation of the Parliament Resolution no. 29/2007[10] regarding the approval for the stationing of the United States of America on Romania's territory concerning the activities stated through the Agreement between Romania and the United States of America regarding the activities of the United States forces located on the territory of Romania, signed in Bucharest, 6th of December 2005, ratified through Law. No. 268/2006

According to art. no. 5 from the Law of national defense of Romania nr. 45/1994[11], modified through the Government Emergency Ordinance no. 13/2000[12], the Parliament Resolution no. 29/2007 was adopted, upon Romania's President's request, stipulating the restriction of the number of members belonging to the United States of America force on Romanian territory. This number was maximum 3000, with the possibility of supplementing it up to 500.

---

[9] *"Poroşenko: placing the Russian missiles in Crimea grows the risk of a major conflict in the Black Sea region"*, Lilia Traci, Agerpres, 19th of March 2015 http://www.agerpres.ro/externe/2015/03/19/porosenko-amplasarea-de-rachete-rusesti-in-crimeea-creste-riscul-unui-conflict-major-in-zona-marii-negre-14-02-22, accessed of the 19th of March 2015;

[10] Document published in Monitorul Oficial no. 294 from the 03rd of May 2007;

[11] Document published in Monitorul Oficial no. 172 from the 07th of July 1994;

[12] Government Emergency Ordinance no. 13 from the 13th of March 2000 for modifying art. no. 5 from the Law of Romania's national defense no. 45/1994. Document published in Monitorul Oficial no. 111 from the 14th of March 2000;

Later on, Law no. 291/2007 concerning the entrance, the stationing, the deploying of operations or the transit of foreign armed forces on Romanians territory was adopted[13]. The law regulates, on one hand conditions that need to be respected on Romanian territory by the foreign armed forces belonging to other states that are not NATO or Partnership for Peace Members, and on the other hand it stipulates juridical measures in applying some orders from the bi and multinational treaties concerning the status of forces.

This document completely changes the conception regarding the presence of foreign armed forces on Romanian territory. If the above mentioned Parliament Resolution would have made any references to the number of military and the amplitude of the operations that take place and if it contained some restrictions concerning the time frame of the applicability of the provisions, the new regulation endorsed a fundamentally different approach. Therefore, all sorts of limitations have been removed concerning the number and the amplitude of the participant forces. Art. 55 from Law no. 291/2007 deliberately abrogates art. 5 from Law no. 45/1994, which stands as the legal base for Parliament Resolution no. 29/2007. Because of the above mentioned abrogation, the legal base through which the president of Romania can address himself to the Parliament asking for the stationing, the deploying of operations or the transit of foreign armed forces on Romanians territory disappeared. One theory was that this resolution became obsolete. Some specialists say that the Parliaments Resolution is still valid. Since there are both pros and cons, it was decided that this juridical document should be drawn to the attention of the Parliament which should decide the path to follow so that its applicability will no longer be valid, as it is in total discordance with the provisions stipulated in Law no. 291/2007, document with de same juridical force, but more recent.

2.3 Signing and ratification of the Supplemental Agreement to the Paris Protocol regarding the status of international military headquarters belonging to the North Atlantic Treaty, signed in Paris 28th of August 1952[14]

So far, Romania did not feel the acute need to legalize this international agreement, where, on one side, is NATO, represented by the Supreme Headquarter Allied Powers in Europe and the Supreme Allied Transformation Headquarter and, on the other side, is the member state.

The treaty refers especially to inviolability, immunities, status of the members, etc. We can see that the project has a chapter dedicated to financial advantages regarding acquisitions, imports and exports, funds, donations, purchasing, fuels and lubricants, the usage of the harbours, airports, etc.

2.4 De lege ferenda regarding Law no. 291/2007 concerning the entrance, the stationing, the deploying of operations or the transit of foreign armed forces on Romanian territory[15]

The first law adjustment should be to set out additional aspects regarding the procedure of approving the establishment of foreign military bases. It must be stipulated who will make the proposal to the country legislative court for admitting the existence of permanent foreign armed forces on the national territory and what kind of notices are necessary. In our opinion the proposal should be made by the President of Romania, as he has the agreement from the Supreme Council for State Defense where he is the president.

We need to enlarge the vocabulary related to the presence of permanent foreign military to avoid the misinterpretation according to which the law contains an enumeration

---

[13]Document published in Monitorul Oficial no. 758 from the 8th of November 2007;
[14] Document published in Monitorul Oficial no. 845 from the 15th of September 2004;
[15] *Ibidem,* pg. no. 5;

strictly limitative – headquarters, military bases or military representation. In our opinion the law should stipulate, in this matter, more general expressions, like "entities" or "structures" that should confer flexibility to the provisions.

The second suggestion is that the law should regulate the "prepositioning" simultaneously with determining a definition for this syntagma. From our point of view, for accurately preparing for operations and for these to work out efficiently, it is necessary for the military personnel, to have in certain public locations, the material and equipment required, even escorted by security personnel, maintenance, transportation, etc. The law must contain references to technical agreements concerning the prepositioning, this stipulation being a legal base for concluding these agreements between the Romanians and foreign armed forces.

A third suggestion has to do with the entrance of foreign forces on our territory by unusual methods, like parachuting. Currently the law refers to crossing the states border "through other place" and this could lead to restrictive interpretations.

A final situation brought into attention is that, due to security reasons, Romania, on its own expense, can provide the foreign armed forces with a number of facilities, products, materials, goods and services, gratis. At the moment, there is no such possibility unless it's against remuneration and it is not debarred for us to offer something free of charge so that we can protect vital interests of the Romanian state.

2.5 Amending the fiscal Code[16]

We are thinking about modifying and supplementing the fiscal Code in order to offer our allies proper conditions for their military personnel to be deployed on Romanian territory, without having to pay discouraging taxes. If the Romanian citizens are obliged by the fundamental law and other laws to pay taxes for the Romanian state, money used for serving its citizens, we cannot demand the same for the citizens of other states, members of foreign forces, allied, who pay their contributions to their states while they are in Romania to help increase the defense capability of our country.

For Romania's sake, they should not be subjected to the fiscal regulations of the Romanian state because they can't be motivated to participate in military missions on our territory. Neither them, nor the states they belong to. It seems fair enough that the Romanian citizens, members of an international headquarter, when acting on duty, to benefit of tax exemptions, facilities, exceptions, etc., just like their foreign colleagues.

2.6 Amending Law no. 346/2006 concerning the organization and functioning of the Ministry of National Defense[17]

The juridical document mentioned above could suffer some modifications or completing that aim for one goal: the strengthening of the cooperation capacity with the allies on our territory, through regulations that endorse a more efficient and pragmatic re-organization of the Army in critical situations, the way the alliance can overtake some command and execution structures of the Romanian Army, as well as the possibility to offer support, free or not of charge, by the Ministry of National Defense for the international defense entities that will be established on national territory.

When referring to re-organization, we mean that a certain subordination of some headquarters established to execute missions has to be flexible rather than rigid like it was in the old theory. This means that military structures have to adapt themselves to new conjuncture. So, the headquarters could be under the command of a central structure, like the

---

[16] Document published in Monitorul Oficial, Part I no. 927 from the 23rd of December 2003;
[17] Document published in Monitorul Oficial Part I no. 654 from the 28th of July 2006;

General Staff, but separated from the force structure, or either inside the force structure, as an element in an army force, or outside of it.

2.7 Others

At this point, we can only anticipate, without accurately predicting, all law amendments necessary for facilitating the founding and developing of activities of the permanent military international entities established with Romania's approval on the territory of this country, with the participation of the allies. Some of the weak points have been identified and they can be subject for some amendments, leaving the list opened.

Obviously, for establishing the NATO Division Headquarter in Bucharest, it will be necessary to sign a Memorandum of Understanding with each participant country, as, for the proper functioning of the NATO force for integration unit, the Alliance will develop a whole architecture of legal documents, taking into consideration that there will be established five structures of this type in different countries.

It is necessary to apply the provisions of the Memorandum of Understanding between the Romanian Government and the two mentioned headquarters at point 2.2. concerning the host nation support for executing NATO operations and trainings.

We don't exclude that, in some ways, we will find the problems along the way and we will come with legal solutions at that time. Our scope is to diminish as much as possible these situations that concur with inherent doubts and confusions, caused by the imminence of the aggression, generating incertitude, instability, panic, chaos. That is why in these times it is imperatively necessary to increase the prediction capacity through maximum focusing and lucidity.

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 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. "If Romania was attacked by Russia", http://qmagazine.ro/ce-nu-se-vede-la-tv/daca-romania-ar-fi-atacata-de-rusia/;
2. "Impetus Putin. The opportunity for a tandem between Romania and Poland", http://www.romanialibera.ro/politica/institutii/stimulentul-putin--oportunitatea-unui-tandem-romania-polonia-370623;
3. "Ioan Mircea Pascu: The military equilibrium from the Black Sea region changed in Russia's favour", http://www.agerpres.ro/externe/2015/03/17/ioan-mircea-pascu-echilibrul-militar-din-regiunea-marii-negre-s-a-schimbat-in-favoarea-rusiei-12-22-03;

4. “Moscow celebrates a year since the annexation of Crimea through a concert-meeting in the Red Square where Vladimir Putin is expected”, http://www.agerpres.ro/externe/2015/03/18/moscova-sarbatoreste-un-an-de-la-anexarea-crimeii-printr-un-miting-concert-in-piata-rosie-la-care-este-asteptat-si-vladimir-putin-11-34-24;
5. “Poroşenko: placing the Russian missiles in Crimea grows the risk of a major conflict in the Black Sea region”, http://www.agerpres.ro/externe/2015/03/19/porosenko-amplasarea-de-rachete-rusesti-in-crimeea-creste-riscul-unui-conflict-major-in-zona-marii-negre-14-02-22.
6. “Russia is replaying the intimidation card. It moves the nuclear weapons closer to Europe”, http://www.paginaderusia.ro/rusia-iar-joaca-cartea-intimidarii-muta-armele-nucleare-mai-aproape-de-europa/;
7. “Stratfor analyzes Romania’s chances in from of Russian invasion”, http://e-politic.ziuanews.ro/dezvaluiri-investigatii/stratfor-analizeaza-ce-sanse-ar-avea-romania-in-fata-unei-invazii-rusesti-168420;
8. “The worse situation crossed by Romania in the last decades. A diplomat and historian, relating about the danger of a war with Russia”, http://stirileprotv.ro/emisiuni/dupa-20-de-ani/e-lucrul-cel-mai-grav-trait-de-romania-in-ultimele-decenii-un-diplomat-si-un-istoric-despre-pericolul-razboiului-cu-rusia.html;
9. „Merkel Promises Support for Baltic States Alarmed by Russia”, http://www.wsj.com/articles/merkel-promises-support-for-baltic-states-alarmed-by-russia-1408383489;
10. Government Emergency Ordinance no. 13/2000 for modifying art. No. 5 from the Law of Romania’s national defense no. 45/1994 published in Monitorul official, no. 111 fro the 14th of March 2000;
11. Law no. 291/2007 regarding the entrance, the stationing, the deploying of operations or the transit of foreign armed forces on Romanians territory, published in Monitorul official, no. 758 from the 08th of November 2007;
12. Law no. 346/2006 concerning the organization and functioning of the Ministry of Defense, published in Monitorul official, Part I no. 654 from the 28th of July 2006;
13. Law no. 362/2004 concerning Romania’s adherence to the Agreement between the Parties to the North Atlantic Treaty regarding the Status of their Forces, signed in London on the 19th of June 1951, and the Paris Protocol regarding the status of international military headquarters belonging to the North Atlantic Treaty, signed in Paris 28th of August 1952, published in Monitorul official no. 845 from the 15th of September 2004;
14. NATO Agrees To 'Readiness Action Plan' To Counter Russia”, http://archive.defensenews.com/article/20140603/DEFREG01/306030034/NATO-Agrees-Readiness-Action-Plan-Counter-Russia
15. Parliament Resolution no. 29/2007 regarding the approval for the stationing of the United States of America on Romania’s territory concerning the activities stated through the Agreement between Romania and the United States of America regarding the activities of the United States forces located on the territory of Romania, signed in Bucharest, 6th of December 2005, ratified through Law. No. 268/2006, published in Monitorul official, no. 294 from the 03rd of May 2007;
16. The fiscal Code from 2003 published in Monitorul official, Part I no. 927 from the 23rd of December 2003;
17. The Law of Romania’s national defense no. 45/1994, published in Monitorul official nr. 172 from the 07th of July 1994.

CREATING A TASK FORCE IN ORDER TO PERFORM A MISSION IN THE GEO-STRATEGIC CONTEXT IN THE PROXIMITY OF ROMANIA

Virgil–Ovidiu POP, PhD
Brigadier General, Associate. Professor, commander of the "UNIREA PRINCIPATELOR" 282nd Mechanized Infantry Brigade.

Ilie MELINTE
Lieutenant colonel, PhD. candidate "Military Sciences", "CAROL I" National Defence University Bucharest, "UNIREA PRINCIPATELOR" 282nd Mechanized Infantry Brigade, e-mail: imelinte@hotmail.com.

Bogdan TUDORACHE
Lieutenant colonel "UNIREA PRINCIPATELOR" 282nd Mechanized Infantry Brigade, e-mail: bogdantudorache28@yahoo.com.

Abstract: *The paper presents the possibilities for establishing a tactical level task force with immediate reaction, able to perform a combat mission.*

Benefiting from the practical activity and from the identified lessons, the authors bring into attention the capabilities of the established force, the present limits and an analysis for diminishing their effects.

The conclusions and proposals support the decisional factors regarding the combat training of these structures and the identification of the subordination/ cooperation relations between the structures which belong to the various categories of forces of the Romanian Army.

Keywords: *transformation, organisation, model, action, reaction, task forces, mission.*

Introduction

The last period was generally the one in which the integrated nature, intercategories of forces of military actions imposed itself. In this period, as a result of the technical and scientific revolution, especially in the field of information technology, various concepts have been issued, describing the military actions as a competition in which the winner is the party involved which better understands the battle space and transfers this knowledge faster to its own fighting units, in order to apply the necessary force with speed and accuracy, at great distances. The success is represented by the use of the fighting power in the interaction and cooperation among the different weapon systems and military structures.

The reduction of the military force and the creation of the fighting structures with design possibilities in any operation area, versatile and flexible, the appearance and use of the new technologies and weapon systems have led to changing the action performance concept, to adopting new JOINT type strategies, as well as to such a preparation of forces in peaceful times.

The land forces shall continue to remain decisive in the joint military actions, especially because the transformation process undergone shall lead to the possibility of them performing the whole range of military actions, land and airborne, independently of location and time.

In the approaches of the content of the new concepts for leading military actions must consider the precision, speed, action range and efficiency of the new military technologies being applied and implemented.

The use of the task forces has as a purpose reaching of the aims in accordance with action plan / order of a brigade.

1. General aspects

The task force can be defined, in principle, as a temporary group of structures (units and subunits) belong to one or more categories of the army forces and branches and, more recently, as a result of the growth of the interoperability level between the Army of Romania and that of the other NATO member states, of an alliance (military coalition) put under a unique command and meant for achieving a battle device for performing a certain mission.

From this definition result that the temporary nature of the task force results, determined by the duration of performance of the mission for which it is established, as well as the high mobility and flexibility of its structure, elements with are determinant for surprising the enemy, in terms of conception and action.

The task forces are created from action needs, in certain situations and conditions and it does not exist as structural entities during peaceful times. They shall be established in the crisis (tension) period and especially for performing certain missions related to collective or national defence, on the national territory or outside it, within agreements, allegiances and commitments undertook by the Romanian Army.

Establishing the task forces, during crisis as well as war periods, is determined by: the structure of the armed forces during peace and wars; the types of missions they undertake; their operational structures according to modules of action groups; the degree of classification, capacity and training of the units and big units; the action needs resulting from the strategic and operative situation; the temporal and space dynamics of military actions; the operationalizing possibilities and conditions of military forces; the ability to regenerate and resize the forces; the technical level of weapons and systems of the forces; the ability of the commandments to create viable solutions, to think, plan and lead military actions.

In the design and performance of the task forces one must adopt efficient solutions, considering the cumulative effect of these factors as, only in this manner, the objectives proposed in the operation can be completed.

In order to establish such a task force on the national territory, it is necessary for the structures which shall be considered to be part of it and comply with the following features:

– mobility and deployability, meaning the ability to rapidly employ them in any operation area on the national territory where they are needed and, in case of need, also outside the country;

– support and self-support – the ability to have the use of own logistic support for at least 30 days; as well the ability to supply them subsequently, for lengthy operations;

– effective engagement – the ability to engage any enemy in the low intensity operations as well as in the high intensity operations;

– the capability to survive – the ability to protect its own forces and infrastructure against the actions of the enemy;

– interoperable communications – the compatible command-control systems in all task force structures, as well as the ones of other military structures, in order to allow them to work and cooperate efficiently together.

The Task Force can be led by the Commander of the Joint Task Force (JTF) at operative level or directly by the CNMC at strategic level. We think the Task Force established on the national territory can be used in the following situation: force

demonstration (to discourage a possible aggression) by a deployment in a certain area / range field or the use as stand-alone force for performing the military operations gathered on the national territory within the national defence.

The Joint Task Force Headquarter role is to ensure a task force, under a unique command, in order to act on the national territory or, according to the commitments taken within the Alliance, outside it. So, in the actual geostrategic context, Romania will have a special role in the NATO.

The need to design and establish a national group of combined forces is determined by the existence of various imperatives which define the evolution of the new present security environment, at the beginning of the third millennium. These refer to the strategic imperative, the technological imperative, the threats imperative and respectively the risk diminution imperative[1].

The strategic imperative for establishing an operationalized group of forces combined at national level is determined by the fact that presently – and much less in the future – we cannot afford acting in an undue manner in case of threats, which means that Romania needs a combined and connected force, defined by increased fighting power, manoeuvrability and agility to act or react, or, as applicable, from a favourable position and to defeat/reject any enemy, and at the same tame perform an active defence of the rest of the national territory.

Through the rapid advance of the modern technology, *the technological imperative*, categorically forces us to perform proper structural changes, as well as to rethink the operational concepts. The task force established in this manner, with a high operationalization level, can be a solution.

Considering that „most threats, challenges or dangers regarding the human society have a hazy profile, which prevents their easy identification and adopting counter-solutions rapidly"[2] one must consider also to the imperative of threats.

The threats imperative identified in the present context also leads us to consider that it is necessary to design one (or many) task forces to handle relatively new threats[3]. Among them: increasing the regional instability and increased asymmetric threats (increasing terrorist actions, purchasing mass destruction weapons, etc.); the takeover of military power by some separatist / nationalist groups, through their sponsorship by certain governments and organizations with interest in the area; the diversity, the large number of sources and unpredictability of the place of conflicts. All this factors determines the impossibility to use a certain type or military force category to defeat an enemy in a specific geographic area.

To respond to the *imperative of risk diminishment*, we can consider that when establishing new combined force structures one must consider that in the next years the risks towards national security can be military as well as conventional, which imposes performing, first of all, operationalized forces and proper instruments able to issue immediate response in the land, air and naval environment and, subsequently, structures with longer operationalization terms.

So, in the present security context, the military action cannot be performed at least in the final moments of the crisis unless by a combined and integrated force, with a big fighting power, flexible and rapidly deployable, able to perform the whole range of fighting, fighting support or established logistic missions, under national command or within NATO. This force

---

[1]Group of authors (led by LTG. (ret.) phd. Eugen BĂDĂLAN), *Present day strategic and operative concepts,* CTEA Publishing House, Bucharest, 2004, p. 32.

[2]BUȚA, Viorel, BG. phd. prof., *EVOLUTION OF THE NATO STRATEGIC CONCEPT – the continuity and flexibility of an alliance in the international security environment*, Military Science Magazine, Edited by the Department of Military Sciences by the Scientists' Academy in Romania, No. 1 (22), Year XI, 2011, p. 53.

[3]Group of authors (led by LTG. (ret.) phd. Eugen BĂDĂLAN), *Present day strategic and operative concepts,* CTEA Publishing House, Bucharest, 2004, p. 34.

could mean the top military structure of the Romanian Army, a completely integrated force, which includes elements of land, air and (eventually) naval forces, highly organized, endowed and trained, capable to act in a combined manner.

Considering all these, we think that the combined task force should respond to the following requirements:

a) structural: high personnel level; operational combat vehicles, techniques and weapon systems, modern and compatible military equipment; high training and interoperability level;

b) actional: high reaction capacity; command, control, communication and intelligence systems capable to assure performing the military actions; the fighting, fighting support and adapted logistic capacity for the whole range of military operations; high degree of logistic independence and self-support.

2. Management of the battle information

The battle field needs for the commanders of each structure to take the proper decisions, supported by information at all levels. At the moment we establish an increase of the quantity of information and it is very important how and what of it we use in the process of planning and leading the forces in the military actions.

The features and requirements of the current military confrontations and the complexity of the present political and military situation lead to the confirmation and grant of a higher attention to the role of the military information for combat and the integration of the military information structures, endowed with modern technique and well prepared, able to plan and perform information collection actions, in order for them to be analysed and disseminated.

The information has a very important role in supporting the military actions, permanently aiming to ensure the information superiority in order to ensure a certain informational support and anticipatory to taking the decision. It comes from specialized or unspecialized, human or technical sources, obtained through specific actions, or through other means available to the commander.

For the commander of the brigade level force tasks in the operation areas it is important that, for the next mission, to know the training level of the enemy's staff, the operational state of its fighting means, the support of the population in the action area are known.

In this context one can identify capacities of the HUMINT[4], IMINT[5] and SIGINT[6] structures, which support the brigade task force, especially in modern conflicts, where the actions are based on effects:

- collecting information;
- protecting information;
- forbidding access to information;
- information management.

For the neutralization or rejection of the enemy, the elements of information structures, as well as the tasks subordinated to the brigade act to influence or control the physical area (space, logistics, manoeuvre, staff or equipment), informational (databases, information flows) and cognitive (understanding, awareness, assessment or decision)[7].

[4] Human Intelligence
[5] Imagery Intelligence
[6] Signal Intelligence
[7] Doctrinaire conference of the Land Forces, Vth edition, 2007, p. 247.

The success of the brigade's mission is essentially influenced by the use of one or more INFOOPS[8] action meas. So, between the enemy's observation and orientation stages it is indicated to use military disinformation and deception, and subsequently, during his decision making being recommended to use PSYOPS[9], so that in the end, during the performance of the military action, electronic war actions will be used.

The brigade's forces, with information support provided by the HUMINT, IMINT or SIGINT aim the exploitation, deceit, influencing or degradation of various categories of targets during the confrontation: command points, communication centres and networks, radars, artillery structures and air defence.

The HUMINT teams supply to the commander of the brigade information about the intentions of the enemy's leaders, which can be used as warnings for the benefit of the force's protection, and in cooperation with the IMINT structures, identifies the key locations of the enemy.

In case the technical means cannot be used for collecting information, the HUMINT teams can represented to whole source of information available to the commander of the task force. In order to have maximum efficiency, in order to coordinate the information collection effort, check their availability and eliminate possible errors, the HUMINT teams must be in continuous contact with the brigade's information structure and with other information, surveillance and research means.

The SIGINT and electronic war structures offer information regarding the battle capacities, arrangement, composition and intentions of the enemy. In addition, it offers information about important objectives in the enemy apparatus, in order to use them in the available fire system. Also it supports the actions of the task force which performs electronic attacks, as well as the electronic protection of its forces and means.

The major contribution of IMINT in performing the brigade's mission is brought by the UAV[10] team, whose technical tools comply with the information needs at tactical level. Within the brigade, these actions target the inspection of the battle field, by day and by night, establishing the coordinates of the targets and the effect of fire on them, the marking / illumination with laser radiations of the objectives in order to hit them with self-guided missiles.

The images obtained through the IMINT platforms often improve the level of understanding of the battle field situation by the general staff of the task force, supporting it in focusing its effort and protecting the fighting power. Except for the direct observation performed by artillery observers and investigation subunits, the images obtained by UAV are the only ones which offer to the commander the possibility to observe the battle field in real time, while the actions are being performed.

Also the central structure command the information structures, it is obvious that must permanently maintaining a perfect coordination with the commander of the brigade level task force. The information collected and sent to the central structure is analysed and subsequently disseminated, according to the „need to know" principle. Still, the imminent warnings are immediately sent to the commander and subsequently to the superior structure, for the preparation of the action orders to the task group. But meanwhile the commander has managed to adopt the minimum measures to avoid the danger.

The commander of the brigades supported with information has the responsibility to perform a proper communication and information technology system, which allows the whole use of the information processed and provided by the information structures or the research subunits.

---

[8] Information Operations

[9] Psychological Operations

[10] Unmanned Aerial Vehicle - type SHADOW 600

The final product of the actions performed by the HUMINT, IMINT and SIGINT structures is the information, which actually represents the knowledge of the battlefield dimensions – physical, cultural, political and moral related, knowledge regarding the enemy and his action possibilities. Due to the technological processes, the accuracy of the research and supervision capacities has grown, which lead to a decrease of the human factor's involvement in obtaining information, in favour of using HI-TECH, respectively the sensors mounted on UAVs. Also, the systems served by the SIGINT structures have become highly efficient, not leaving to the enemy many chances to use the communication systems completely safely. The only exception is given by the HUMINT structures, which remain an important source of information obtained through methods inaccessible for technical systems.

For the commander of a brigade level task force, which acts independently or in a superior echelon, the information received from their specialized collection structures is an important support in taking desirable decisions and is an essential element of the military actions performed for using the fire power of the subordinated forces and means, especially due to the fact they target what most of the times constitutes the enemy's centre of gravity, precisely the command and control system.

The brigade must have information to successfully perform the military actions. These must be relevant, essential, desirable and presented in an accessible form, to be understood and rapidly used by the attack forces, to act in an optimum manner for the performance of the missions.

3. Battle organisation

The changes of form and content which configure today's conflicts impose that the military reform promotes the creation of elite forces formed from units selected and trained at strict standards, endowed and organized according to the missions preferred to be received and, not last, which have and continue to improve their battle experience.

It is probable that in the future the mass armies shall continue to accomplish those clear purposes (intimidation, pressure, obtaining unconditional success against the smaller or less equipped). We note that more and more often, in case of extension of uncertainty situations, respectively amid the indecisions and prompt amplitude reactions, the small, professional groups and which are guided according to attentively commanded plans have become able to destroy the enemy or obtain the anticipated success without being in direct conflict.

We want to highlight here the fact that in the establishment and in the involvement manner in the military actions of a task force, especially of one at brigade level „an attentive analysis of the operational environment and of the evolutions of the adversary's action manners is imposed, which can guarantee maintaining the efficiency of the structure in the operations performed."[11]

Continuing to argument the above, we bring in discussion the two complementary aspects on which the efficiency of a military structure of a battle field is based: organisation for battle and training.

Talking about the organization for battle, it is known that in the case of a brigade level task force in our army we can talk about two organization manners and the use of the component structures: the classic one, in which the units and subunits are employed in the standard format and the one of mission organization, respectively under format of battle groups.

[11]MITULEȚU, Ion, COL. phd. prof., *Mechanized brigades (infantry, mountain troops). General principles, organisation, place, role, destination, principles of use in the battle, general information related to operations – Academic class* MILITARY ART LAND FORCES, National Defence University „Carol I", 2012, p. 12.

The analysis of the conditions in which it is decided to use the forces in the manner of battle groups, different from the classic one, has multiple motivations. Here we refer to primary aspects, such as the answer requested at 5 „W" (who, what, when, where, why?) as well as to the extended aspects regarding the need to model the tactics and adaptation of battle systems in the special conditions of a tactical situation.

The establishment of battle works implies the detailed analysis of the needs and possibilities, on which the optimum organization of manoeuvre forces, battle and logistics report reported to the mission which has to be performed is based [12]. The ideal case implies that the assigned resource is reinforced in proportion to mission to be accomplished, respectively with the threat. But reality makes us consider the fact that the forces and means of the brigade are limited, in the situation of establishing a task force, the base is composed by the force structure and means available at that moment.

The main purpose for establishing the task forces is to support the conception of the action, especially in relation to its course and the efficient engagement of the brigade level task force in operations. The activities performed for establishing the battle groups keep into account the following factors:

- the structure of the brigade and of the elements received from other echelons;
- the level of classification and endowment of the structures;
- the specific of the brigade and the missions in which it can be engaged;
- the effects and action needs resulting from the analysis of the situation;
- the time/space criteria of the military action;
- the flexible elements of the logistic system.

The major advantage of the battle groups must be determined by the synergy created through the weapon group for a specific mission. The mission organization means that the battle groups are able to regroup fast (in any seasonal conditions, weather, by day and by night) in the operation performed and that they are composed of subunits trained together, things which concur to the success of the engagement in the operation.

Moreover, based on the experimentation during the drills performed in polygons, we have noted that in the case of any group, the whole potential of battle groups can be developed and improved only through collective training and the command unit manifested at the highest degree of discipline.

Here we are considering the two principles which must be fully understood and implemented in all echelons: the manoeuvre approach and the command of the mission (already included in the doctrine of Land Forces).[13]

By developing these principles we support the idea according to which the offensive actions must be adopted whenever the opportunity arises, complying with the conception of maneuver of the direct commander and respecting the intention of the one two echelons higher. The battle groups must develop and must bear such a high rhythm of the operation, element which is reached only through effective training, strong leadership, a common doctrine, common drills, a solid logistic ground and the efficiency of the procedures on the battle field.

Usually a battle group organized within the mechanized brigade includes:

- the commander of the battalion, around which the force is organized;
- up to 5 manoeuvre subunits, usually composed of infantry and tanks;
- one research subunit;
- up to 3 units to support the manoeuvre (Artillery, including Anti-Tank weapons);

[12]MARTIN, Iulian, phd., *The structure, missions, training and certification standards of European battle groups*, in STRATEGIC IMPACT No. 4[37]/2010, Publishing House of the „Carol I" Defence University, Bucharest, p. 86.
[13]FT 1 / 2007 - The Land Forces Doctrine.

– one air defence subunit;

– an engineering structure to which the organization of the weapon specific means for the mission shall be added;

– logistics: logistic support squad, part of the logistic of the „mother" unit for each subunit, a medical subunit.

The principles for using the mechanised brigade or a task force of this level in the operation are: action in all types of fields; managing to take by surprise; involvement in decisive actions; use in manoeuvre actions in large spaces; modular use; efficient and advisable support. Each of the mentioned principles must be acquired by the brigade commander before taking the decision regarding the organisation of the forces on battle group type structures.

Looking at „how many" such groups can generate a mechanized brigade, we note that one can form as many battle groups as battle units subordinated to it, as the regrouping shall take place around those commandments. Battle groups can be organized, exceptionally, under command of ad-hoc created commandment in the battalions or superior echelons.

Still the availability comes from the fact that different battle groups can be organized: stronger, easier or balanced, feature related to the number of tank and infantry subunits included in them. The organisation shall be decided according to the mission of the brigade in the superior echelon, to the results obtained from the analysis of the mission, to the manoeuvre adopted and event to the results of the war games.

Other motivations or situations to which the decisions of forming the battle groups at the mechanized brigade level are based are the external ones: at the order of the superior echelon and the one imposed by the situation at the forces at a certain point (losses, assignments, resubordination etc.).

In the first case we have the situation in which the brigade receives an order to provide to the superior echelon forces up to the value of one unit, for the performance of some tasks.

The second is the situation in which the brigade commander can be obligated to perform the reorganisation of the forces, as a result of independent actions of his command (losses, destructions), in order to continue the battle or perform battle tasks using the available forces.

Although one might consider that the „battle group" replaces the old „squad", the arguments regarding the difference are given by features and purpose. In the first case we have the high degree of independence, the higher manoeuvre role, the independence in actions and increased possibilities to obtain the desired effect of the battle power. In relation to the squads, according to the specialty literature, they are mostly organised for one action, precise and usually lead by the superior echelon.

The command and control in a battle group are not different from the regular military structures, in this case only features resulting from the increased independent nature of structures and maybe from the specific limitations regarding using forces with a special status in battle appear.

The commander of the battle group maintains the organisation of the battalion commander on which it's formed but it is necessary to enlarge it with specialists in using the forces, which come to complete it, other than the ones available to that unit. From the practice in the brigade we have concluded that the presence of the specialists is necessary for the use of the structures coming from outside the mechanized brigade or the battalion, such as: aviation, tanks/infantry, artillery, ISTAR, CIMIC, PSYOPS elements).

Another element derived from the experience of the combat missions and of applications is that the efficiency of a battle group significantly depends on the commander's personal abilities and personality, elements highlighted in all activities.

4. Training

The training of the troops must complete some conceptions of the operations which emphasize the unforeseeable and fighting against it. During the trainings, the troops and general staff must be put in situations as less familiar as possible and forced in order to think in a creative manner.

The aspects presented above initiate the creation of an image regarding the manner for establishing battle group type structures, but we must highlight that in order to ensure the criteria of decisive engagement in the operation of the components as well as the whole brigade level task force, the training component must be applied very accurately. The training of the structures must be efficiently oriented towards the development or improvement of the features specific to a credible force, such as mobility, fire power, flexibility, self-support capacity and which offers the ability to perform any mission entrusted.

An important step in the force training field is the implementation of the scenario, respectively of the unique application of the whole category of land forces. We think that the implementation of this decision is advisable not only because it ensures an imperative need given by the military situation in the proximity of our country, but also because it is based on a rich testing and application activity performed in the last years.

We refer here to the activity of the Brigade 282 Mechanized Infantry where, starting with the training year 2008, the variant of the "unique scenario" was proposed and applied, with the precise purpose to improve and perfect the conception and ensure the proper tactical framework for the drills, training camps and tactical applications performed by the great unit and by the subordinated units (for any echelon, until and including the brigade) for one year.

The success of the „ unique scenario" was well understood by the whole category of forces which determined, in the following years, in all brigades, to sketch a general tactical framework, which answers to their training objectives and requirements, according to the missions and their destination, the performance level reached, implicitly the competences and action capacities specific for the structures involved.

The unique scenario represents „the general tactical framework in which the training for units and great units is integrated, which ensures an unitary and modern performance conception and which is used to answer to the training requirements of the unit and of the great unit"[14]; it has a high degree of complexity, but also offers flexibility to the commanders in the planning and performance processes.

This organization and preparation variant for the scenarios for tactical exercises and applications, applied during one year of training ensures a unitary conception for the approach of the training and drill process.

The value of this idea has increased exponentially each year, which is noticed through the nature and amplitude of the drills with troops on the field, performed by mechanized brigades, features which have trained without doubt every type of operational structure in the land forces, but also the ones in the other categories of forces.

The series of advantages of the unique scenario and which made it a solution in approaching the training process of the whole force category in the past year includes the following:

– ensures the joint[15] and combined[16] through the manner in which the stages of the application are performed and prepared. So, one can include all the specific stages for the

[14]TOMESCU, Cătălin, T., Gl.bg., Dr., Doctoral thesis: *Opinions regarding the training of Land Forces in the context of their attendance to managing national and global military conflicts*, National Defence University „Carol I", Bucharest, 2010, pp. 146-147.

[15] The specific weapons and branches for a force category

[16] Inter-categories of armed forces

participation of a task force to a military action (period for increasing the operation capacity, the combined movement in the operating stage, performance of the military actions specific to armed battles, followed by the asymmetric or stability ones);

– it can be easily adopted in training the forces for the performance of military actions on the national territory or outside it;

– at the mechanized brigade level, it ensures coherence in complying with the objectives of the drills and of the training objectives and the unitary nature of the conception (targets the overall forecasted military action);

– ensures the systematic coverage of the themes, by going with the trained structure through all stages and phases, from activation to recovery;

– ensures to the commanders (of any echelon) a high flexibility, offering them the possibility to choose the set of exercises without fear that they could deviate from the objectives of the training year and remain correlated with the immediate national and allied requirements;

– simplifies the activity of the brigade and battalion general staff and cultivates the initiative regarding the implementation of own training conceptions;

– lays down the general frameworks, ensuring the correlation with the national and NATO training objectives and allows the development of any type of military action, in national or multinational format;

– allows repeated training and implementing the lessons learned during the army specific trainings, as well as during the joint and combined action, for all types of units.

This variant is required as binder between the categories of forces (land, air and naval) but also as solution in applying a coherent formula for ensuring the training of the task forces which are active or which can be formed according to the immediate needs related to the country's security. Surely the unique scenario shall be adapted based on the battle experience, on the specific missions and on the objectives of each structure and each commander, improved based on the lessons learned and of the experience achieved by applying it each year and by participating to external operations.

The importance of optimizing the training for the land forces was required each year or stage, always having as main objective preparing the forces in order to perform the whole range of military actions in joint and combined operations on the national territory or outside it. The two major valences in this case are: performing the operational capacities necessary for the participation of collective defence missions, type art. 5, within the NATO structures, and ensuring the security of Romanian's space through limited battle actions and seize actions in the area of responsibility.

Conclusions

For a better approach of the tactical training between the two fields, individual and collective, the unique scenario supports all training structures by systematically establishing the training themes according to the scenario adopted for the training year (oriented on the main battle forms, defence or offence), ensuring reaching the training level anticipated for successfully attending a certain type of operation. This was prepared in detriment of the previous styles, where the structures had the obligation to go through the whole range of military operations, but without reaching a maximum level of training specific for a certain type of military action.

In this context, we appreciate the manner in which the tactical commanding and/or troops exercises and applications, in joint and combined format was imposed during the performance of the training forces, within the Land Forces. Moreover, we have noticed the opening and interest of the other categories of forces regarding the participation to the

important activities of the Land Forces, but also focusing the efforts for bringing the combined training to the level of compulsory condition for the performance of the commandment exercises and of the applications.

The common training activities bring added value for all categories of forces and ensure the performance of the objectives regarding the insurance of security, at national as well as ally level. In the mechanized brigade the performance of combining the exercises at the level of task forces, of the Land Forces (battle group – on battalion structure level) with the exercises of the aviation structures was reached, the suggestive examples being the exercises MĂLINA 14, DANUBE EXPRESS 14 and WIND SPRING 15, activities with advanced joint and combined actions and with multinational participation.

We support the idea that the combined aspect must be practiced also at the lower levels, respectively task force – at company level. For example, the training of attack helicopters, whose basic mission is the fire support of the structures in the Land Forces, which have accelerated the common training with the units and subunits of mechanized brigades. The progresses achieved at the last exercises in range fields have ensured access towards perfecting the performance methods of the close air support in the main forms of armed combat.

The implementation of this procedure has significantly increased the decision process, and has already produced a fundamental change in the planning, performance and assessment of the common exercises Land Forces – Air Forces, performance of the tactical applications (from the company level to the brigade level) in combined frame being a compulsory condition.

The combined training activities are started this year also in relation to the Naval Forces, especially for the structures of Land Forces dispatched in Dobrogea and of the ones which are in direct cooperation to the Danube Fleet structures. This was insured also by adopting the unique scenario of the exercises.

The integrated nature of the unique scenario applied in the whole army offers a special opportunity, well noted and used by the training and doctrine chiefs, respectively the connectivity of the national with the allied drills (the ones of a NATO partner or multinational). This ensures the real reach of the inoperability level of the force groups generated nationally necessary for participating at allied system operations, as well as the possibility to practically check the reaction of these groups and the allied forces to the appearance of imminent threats or for solving military aggression situations.

In this manner we have the bridge between the national efforts and the efforts of the partners in the Alliance to prepare the structures meant to perform the fighting missions according to the strategic concepts and the commitments taken.

All the above proves not only the efficiency of implementing a combined system for performing the training, through exercises and applications for the three categories of forces, but actually the principle of the combined action inherent in case an aggression appears against our country or against another NATO member country.

Aknowledgement:

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. ***, CRISIS, CONFLICT, WAR Volume IV: Military and civil-military systems used in managing crises and conflicts. Dangers, threats, risks towards them. Assessment and testing criteria and methodologies, Publishing House of „Carol I" Defence University, Bucharest, 2007.
2. ***, Doctrinaire conference of the Land Forces, Vth edition, 2007
3. ***, FT 1 - The Land Forces Doctrine.
4. ***, Training in the Land Forces in 2015.
5. BUȚA, Viorel, (ret.) BG. phd. prof., EVOLUTION OF THE NATO STRATEGIC CONCEPT – the continuity and flexibility of an alliance in the international security environment, Military Sciences Magazine, Edited by the Military Science Department of the Scientists' Academy in Romania, No. 1 (22), Year XI, 2011.
6. FRUNZETI, Teodor, (ret.) LTG phd. prof., National power and military power in "THE WORLD 2011 – Political and military encyclopaedia (strategic and security studies)", Technical Centre Publishing House - Army Editorial, Bucharest, 2011, p.21.
7. Group of authors (led by (ret.) LTG. phd., Eugen BĂDĂLAN), Present day strategic and operative concepts, CTEA Publishing House, Bucharest, 2004
8. MARTIN, Iulian, phd., The structure, missions, training and certification standards of the European battle groups in STRATEGIC IMPACT No. 4[37] / 2010, Publishing House of „Carol I" Defence University, Bucharest.
9. MITULEȚU, Ion, (ret.) COL. phd. prof., Mechanized brigade (infantry, mountain troops). General principles, organization, role, destination, principles of use in the battle, general information related to operations – Academic class MILITARY ART LAND FORCES, National Defence University „Carol I", 2012.
10. TOMESCU, Cătălin, T., BG phd., Doctoral thesis: Opinions regarding the training of Land Forces in the context of their attendance to managing national and global military conflicts, National Defence University „Carol I", Bucharest, 2010.
11. www.buletinul.unap.ro.
12. www.cssas.ro.
13. www.dresmara.ro.
14. www.impactstrategic.ro.
15. www.infocercetare.ro.
16. www.strategii21.ro.

APPLICATION OF SYSTEM DYNAMICS IN THE PROCESS OF SHARING MILITARY CAPABILITIES

Antonín NOVOTNÝ, PhD
Colonel (Ret), Ing., assistant professor, Centre for Security and Military Strategic Studies, University of Defence, Kounicova 65, 662 10 Brno, Czech Republic,
e-mail: antonin.novotny@unob

DALIBOR PROCHÁZKA
LtC (Ret), RNDr., CSc., assistant professor, Centre for Security and Military Strategic Studies, University of Defence, Kounicova 65, 662 10 Brno, Czech Republic,
e-mail: dalibor.prochazka@unob.cz

Abstract: *The article describes the application of system dynamics in the process of military capabilities sharing. The aim is not to cover the problem in all its aspects, but to focus on the process of multinational capabilities sharing with emphasis on the Armed Forces of the Czech Republic. Solving problems in capabilities can be achieved by properly-designed investments in upgrading, by improving the NATO defence planning process and accordance with national defence planning process, by consistent execution of capability targets that this process generates, but also by use of multinational capabilities sharing. Pooling and sharing capability among individual member states can have a significant impact on the way to replace the missing defence sources or how to effectively use increasing of defence budgets, which the Alliance, including the Czech Republic, declared at the summit in Wales.*

Keywords: *Smart Defence; Pooling and Sharing; Connected Forces Initiative; Framework Nations Concept; military capabilities; dynamic model.*

Introduction

„To maintain and develop defence capabilities, multinational solutions can be sought through NATO's smart Defence and the EU's Pooling and Sharing initiatives – particularly within the framework of regional cooperation, through closer coordination of defence planning and common development of military capabilities. International initiatives provide opportunities for the Czech Republic to maintain specific military capabilities; however, they cannot substitute for the primary responsibility of the state for national defence and development of its own defence potential. "[1]

In early September 2014, in Newport, Wales, the NATO summit took place, which the previous Secretary General of NATO called one of the most important in the history of the Alliance.[2] Since the last NATO summit held in Chicago in 2012, for the first time in this constitution met the main representatives of 28 Allied states and governments. The original program of this meeting with a particular emphasis on the completion of ISAF and other responses to the increasingly declining defence spending of European NATO countries[3] had to

1MoD. Defence strategy of the Czech Republic. Prague, December 2012. Accessed on 2015-03-10. ISBN 978-80-7278-606-0. Available at web address: http://www.army.cz/images/id_8001_9000/8503/STRATEGIE_an.pdf

2Statement NATO SG A. Fogh Rasmussen before NATO summit in Wales. Accessed on 2015-03-10. Available at web address: http://www.theguardian.com/world/video/2014/sep/04/nato-summit-newport-most-important-in-alliance-history-video

3Total defence spending of 26 EU Member States represented in the EDA in real terms has been declining since 2006. In the period from 2006 to 2011 it fell by EUR 21 billion (almost 10%) and between 2011 and 2012 it decreased even further by almost 3 %. EDA. Defence Data 2012 Brussels, 10 December 2013.

be redesigned with regard to the international political situation. The Ukrainian crisis and the behaviour of the Russian Federation represent a fundamental change in the security environment in Europe and therefore a change of the assumptions on which the Alliance is prepared to fulfil their tasks.

In the last decade NATO focused mainly on its stabilization mission and the fight against terrorism, but a threat to conventional confrontation has now re-emerged. In the future, the Alliance must be able to quickly, flexibly and decisively enough respond to the challenges and risks posed by the current Russian Federation in particular. However, the hybrid method based on asymmetric warfare and at first glance illegible tactics of struggle may in the future be used by other participants. Alliance responses to these threats are a series of measures to strengthen collective defence and capabilities contained in the Readiness Action Plan.[4] The document discusses strategic implications for NATO arising from a changed security environment and presents a set of measures, the purpose and goal is to reassure Allies about the validity of commitment to a common defence. Furthermore, the Readiness Action Plan should adapt Alliance in order to be able to deter or react promptly and effectively to any action that might compromise the security of the Allies. Although the Action Plan was primarily due to the need to respond to Russian aggression, the benefits of its implementation will also be useful for a possible response to all other potential threats, e.g. from the Middle East or North Africa. For the Alliance‘s ability and readiness to face these current as well as future security challenges is an essential condition for the need to have adequate military capabilities. The Alliance has long-term problems in the fulfilment of some of their abilities shortcomings and in defence spending, which has been below 2% of GDP, which have been agreed with the Allies.

At present, only four countries[5] out of 28 members of NATO defence expenditures reach their recommended two percent. It was therefore a very important part of the discussions in Wales and commitment to halt this decline and move towards two-percent threshold, with the objective of achieving over the next decade. At the same time, the member countries also committed themselves to take advantage of increased spending to address major shortcomings in the capacity allocation and 20% of the defence budget on investments.[6] Fulfilling this commitment should lead to stopping the decline and starting the process of increasing defence budgets with the aim of gradually eliminating the imbalance between the US and EU member countries and the equitable burden of defence spending. In this context, the summit also approved a package of defence planning, which sets out 16 priority capabilities that must be developed in order to meet the Alliance’s ambition of NATO Forces 2020.[7]

1. Alliance instruments used to remove shortcomings in the defence capabilities

One of the possible ways to replace the shortfall in European defence spending while maintaining existing military capabilities of the Alliance or at least slow their decline is the use of international cooperation in the development of military capabilities. Multinational cooperation can be implemented across the lifecycle capabilities. Likewise, cooperation may occur at different intensity - in coordination of capabilities and increasing interoperability,

Accessed on 2015-03-10. Available at web address: http://www.eda.europa.eu/info-hub/news/article/2013/12/10/defence-data-2012

4 NATO HQ. Press Release. *Wales summit Declaration.* Article 5. Brussels, September 2014. Accessed on 2015-03-10. Available at web address: http://www.nato.int/cps/en/natohq/official_texts_112964.htm

5 USA, Greece, Estonia, Great Britain

6 Ref 4, Article 14.

7 NATO HQ. *Summit declaration on Defence Capabilities: Toward NATO Forces 2020.* Brussels, May 2012. Accessed on 2015-03-10. Available at web address: http://www.nato.int/cps/en/natohq/official_texts_87594.htm?mode=pressrelease

sharing the role without creation of common structures, the creation of joint structures for the use of national capabilities or the building of shared competence. The common denominator of these activities should be an effort to increase interoperability and efforts to achieve savings in human, material and financial resources. A crucial role in this process is played by adequate political support and will by countries involved and the need to bridge the contradiction between the political declaration and a real willingness to move to the intensive international cooperation in specific areas sharing military capabilities. Coordination of multinational cooperation is a difficult and long process, which often lacks sufficient degree of transparency and can create space additional costs. While multinational cooperation certainly cannot be considered as a flawless tool of development of capabilities and although specific outputs are not currently too strong, it represents by a considerable number of countries a feasible way to ensure their defence in the future. Currently Alliance uses the following means:

1.1. Smart Defence (SD)

Smart Defence Initiative - the Alliance seeks to mitigate the impact of the lack of funds to maintain and develop the necessary allies' capabilities. Involvement in this initiative makes more efficient use of unique national capabilities and access to skills, which independent states are unable to create by themselves for financial and technological reasons. The first list of Smart Defence joint projects[8] was formalized at the NATO summit in Chicago in May 2012. There are currently around 150 projects, divided into three levels - Tier 1, 2 and Tier 3 projects. At present, the most promising are highly developed consolidated projects with a leading country that has been determined – called Tier 1 projects. The participants are at least two countries, which have a clear aim and content and an identified sponsor in NATO.[9] For proper functioning of the initiative it is especially necessary that it is consistent with the requirements of NATO defence planning and to be fully complementary with the activities implemented under similar initiatives of the European Union, Pooling and Sharing, which the Alliance at the summit again supported. [10]

1.2. Connected Forces Initiative (CFI)

The aim of the initiative, announced at the Summit in Chicago,[11] is to maintain a high interoperability of allied forces and revive the alliance's ability to conduct the full range of operations. The core of the initiative is training and education, increasing the number of exercises and better use of technology. The importance of exercise and the need to strengthen the ability of the joint effective work gains importance especially in times of phasing operational tempo after the end of the ISAF operation in Afghanistan. Joint exercises are also demonstrations of credibility of the forces to the outside world. Nevertheless, CFI success depends on the willingness of Member States to allocate the necessary resources in training, exercises and technology. Implementation of CFI is vital to sustain the pace of transformation, interoperability of NATO forces and their operational readiness and effectiveness in post-Afghan period and in the context of the Ukrainian crisis.

---

8 NATO HQ. Multinational Projects. Brussels, November 2012. Accessed on 2015-03-10. Available at web address: http://www.nato.int/nato_static/assets/pdf/pdf_2012_10/20121008_media-backgrounder_Multinational-Projects_en.pdf

9 NATO HQ. Multinational Projects. Brussels, June 2014. Accessed on 2015-03-10. Available at web address: http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2014_06/20140602_140602-Media-Backgrounder_Multinational-Projects_en.pdf

10 Ref 4, Article 70.

11 NATO HQ. Connected Forces Initiative. Brussels, September 2014. Accessed on 2015-03-10. Available at web address: http://www.nato.int/cps/en/natohq/topics_98527.htm

1.3. Framework Nations Concept (FNC)

FNC[12] concept was approved by defence ministers of NATO member countries meeting in June 2014, and should allow smaller states to capitalize on their skills and specialization in larger multinational task forces. The concept of a "framework country" is not new, but has been working in the areas of procurement capability (SD) or generating capacity (e.g. EU Battle Group). The FNC idea deepens and extends the area of planning abilities, mainly the area of the implementation of the objectives assigned under the NATO Defence Planning Process (NDPP). The idea is that the framework country gathered around itself "willing and able" European countries and thus provides a conceptual and organizational framework for multinational cooperation. However, FNC does not create a new link between NATO and the Member States because the objective of NDPP will continue to be allocated to the states. The states will be able to use the idea of being allocated to clusters in order to fulfil of the objectives in a multinational framework. The clusters would thus produce a comprehensive set of capabilities (Capability Clusters) and play a coordinating role. FNC can therefore be considered primarily as a tool for multinational cooperation aimed to meeting the objectives of capabilities development in order to meet the Alliance's ambition level, because there are currently no European allies able to meet fully the desired objectives. Implementation of this concept should be one of the ways to strengthen Europe's defence capabilities and to achieve the NATO Forces 2020 goals.

One of the possible ways to better understand and mitigate the possible discrepancies in the military capabilities pooling and sharing process is modelling and simulation. We used a system dynamics approach. System dynamics (SDy) is a method to describe, model, simulate and analyse dynamically complex issues and/or systems in terms of the processes, information, organizational boundaries and strategies. Quantitative SDy modelling, simulation and analysis facilitates the (re)design of systems and design of control structures. SDy is in fact the application of the principles and techniques of control systems to organizational and social-economic-environmental problems. SDy starts from the assumption that the behaviour of a system is largely caused by its own structure. System structure consists of physical and informational aspects as well as the policies and traditions important to the decision-making process in a system. Hence, in order to improve undesirable behaviours, the structure of the system needs to be changed. SDy allows identifying desirable system changes and testing them in a "virtual laboratory."[13]

The applicability of system dynamics to Pooling and Sharing is given by foundation of the capability building process, where resources are accumulated and transformed into a capability, and where a capability's potential decrease occurs, caused by equipment wear and becoming outdated or by personnel leaving etc. It means that keeping a certain capability level requires adequate resources.

2. Qualitative model of military capability sharing

Evaluation of a capability is important for capability planning and building processes. It provides a base for the Czech Army's capabilities building as well as for inputs to international activities. According to DOTMLPFI methodology (Doctrine, Organisation, Training, Material, Leadership, Personnel, Facility, Interoperability), during the planning processes, functional areas capabilities are considered. This facilitates comprehensive structured description of required changes of the existing state. It is obvious that the capability evaluation has a multi-criterial

12 NATO HQ. Improving NATO´s capabilities. Brussels, February 2015. Accessed on 2015-03-10. Available at web address: http://www.nato.int/cps/en/natohq/topics_49137.htm?selectedLocale=en

13 Pruyt, E. *Small System Dynamics Models for Big Issues: Triple Jump towards Real-World Complexity.* Delft, TU Delft Library 2013. ISBN: 978-94-6186-195-5.

character, but as a simplification, we assume that the capability level can be characterized by a non-negative value.

The modelling process means creating a simplified image of reality, i.e. the model that is further investigated and, based on its behaviour, enables drawing conclusions related to reality. The modelling process is devoted to our purpose, related to investigating phenomena, and it is necessary to critically assess the level of simplifications we have made. The modelling process usually runs in loops, when model behaviour is compared to our assumptions or to the reality and the model is corrected by means of changing its structure (if necessary) or its parameters. The model described in the paper is in this context the initial model made with the aim to verify applicability of system dynamics methods to the topic of building and sharing military capabilities. Thus, only main aspects are reflected in the model.

During the modelling process, following assumptions had been made:

- Only bilateral capability sharing is modelled.
- The model is asymmetric. One participant is a provider (denoted by CZ[14]), the other is a pure recipient (denoted by AL).
- A primary motivation to pooling and sharing is an economic profit. We assume higher effectiveness of the provider in capability building. The will to share or to accept a capability depends on an economic profit.
- Other "soft" factors, such as sovereignty and the will to receive the capability, which influence the pooling and sharing, are incorporated.
- A capability can be shared for other reasons than a direct economic profit; this is reflected by a political will to share the capability.
- Another parameter is trustworthiness, given by fulfilling of declared obligations – providing the declared capability by the provider and (financial) contribution to the capability building by the recipient and by other factors not dependant on the on actual cooperation.
- The model presented below is qualitative, when the focus is on qualitative assessment of system behaviour, not on quantification of model parameters and outputs.

A military capability can be, roughly simplified, characterized by a non-negative value. To reach some capability level and to maintain the level, resources are needed. This relation can be described by means of a stock and flow diagram,[15] see Figure No.1. The relation between the capability$CAP(t)CAP(t)$, inflow $ResourceInflow(t)ResourceInflow(t)$, and outflow $CapabilityDecrease(t)CapabilityDecrease(t)$ can be expressed by equation

$$CAP(t_k) = CAP(t_0) + \int_{t_0}^{t_k} ResourceInflow(t) - CapabilityDecrease(t)dt,$$

$$CAP(t_k) = CAP(t_0) + \int_{t_0}^{t_k} ResourceInflow(t) - CapabilityDecrease(t)dt, \quad (1)$$

where t_0t_0 and t_kt_k are initial and final time values and

$$ResourceInflow(t) = EffectivityCoefficient \cdot Resources(t)$$

$$ResourceInflow(t) = EffectivityCoefficient \cdot Resources(t), \quad (2)$$

$$CapabilityDecrease(t) = DecreaseCoefficient \cdot CAP(t)$$

$$CapabilityDecrease(t) = DecreaseCoefficient \cdot CAP(t). \quad (3)$$

14 The denotation CZ (Czech Republic) and AL (Ally) refers to a hypothetical capability provider and a hypothetical capability recipient without any connection to real countries.

15 The Causal-Loop Diagram of the model is presened in: NOVOTNÝ, Antonín. PROCHÁZKA, Dalibor. Application of System Dynamics in the Process of Sharing Military Capabilities. Defence and Strategy. 2014, Volume 14, No. 2, pp. 87-104. ISSN 1802-7199. Accessed on 2015-03-10. Available at web address: http://www.obrana-astrategie.cz/cs/archiv/rocnik-2014/2-2014/clanky/aplikace-systemove-dynamiky-v-procesu-sdileni-vojenskych-schopnosti.html#.VSUdZJO2o80

Equation (1) describes a generic capability as a dynamic variable – accumulation (stock).

The centre of the model is a partial model of capability building, see

Figure No. 2. It incorporates a negative feedback, where a difference between a required state and an actual state of the capability is generated – the variable$DeficiencyCAPCZ$ $DeficiencyCAPCZ$. Based on the difference, request for finances $RequiredFinResourcesCZ$ $RequiredFinResourcesCZ$ is generated. Following the loop, allocated financial resources are transformed into resources applicable to capability building, (e.g. material, personnel, etc.). The same model is used for the recipient's capability building, where we suppose less effectivity.

We can model the economic profit of capability sharing as the profit directly proportional to finances provided by the capability recipient to the capability provider, from which we have to subtract direct expenses spent by the provider on the capability sharing project.

The sharing policy is an implementation of a capability sharing mechanism. Our aim is not a formulation of a sharing policy at this stage. To verify the basic functionality of the model we assume the capability sharing proportional to expenses spent on the shared capabilityCAPCZ CAPCZ:

$$SharingPolicy(t) = \frac{AccumulatedExpensesCZ(t)}{AccumulatedExpensesALCZCAP(t)+AccumulatedExpensesCZ(t)}$$

$$SharingPolicy(t) = \frac{AccumulatedExpensesCZ(t)}{AccumulatedExpensesALCZCAP(t)+AccumulatedExpensesCZ(t)}, \quad (4)$$

where $AccumulatedExpensesALCZCAP(t)AccumulatedExpensesALCZCAP(t)$ means the recipient's expenses spent on the provider's capability and

$$CAPCZCZter(t) = CAPCZ(t) \cdot SharingPolicy(t)$$

$$CAPCZCZter(t) = CAPCZ(t) \cdot SharingPolicy(t), \quad (5)$$

$$CAPCZALter(t) = CAPCZ(t) \cdot \big(1 - SharingPolicy(t)\big)$$

$$CAPCZALter(t) = CAPCZ(t) \cdot \big(1 - SharingPolicy(t)\big). \quad (6)$$

The meaning of $SharingPolicySharingPolicy$ is the ratio of the capability distribution between the provider and the recipient at time. The value $SharingPolicy = 1SharingPolicy = 1$ means that the provider disposes of all the capability, $SharingPolicy = 0SharingPolicy = 0$ means that the all capability is provided to the recipient. Equations (4) – (6) mean that the actual value $CAPCZ(t)CAPCZ(t)$ in time t_1t_1 is distributed proportionally to expenses spent up to time t_1t_1, i.e.

$$AccumulatedExpensesALCZCAP(t_1) = \int_{t_0}^{t_1} SpentFinResourcesALonCZCAP(t)dt$$

$$AccumulatedExpensesALCZCAP(t_1) = \int_{t_0}^{t_1} SpentFinResourcesALonCZCAP(t)dt, \quad (7)$$

$$AccumulatedExpensesCZCAP(t_1) = \int_{t_0}^{t_1} SpentFinResourcesCZCAP(t)dt$$

$$AccumulatedExpensesCZCAP(t_1) = \int_{t_0}^{t_1} SpentFinResourcesCZCAP(t)dt. \quad (8)$$

The provider spends his resources only on capability$CAPCZCAPCZ$, while the recipient can distribute his resources between own capability $CAPALCAPAL$ and shared capability$CAPCZ$ $CAPCZ$, depending on his sovereignty and other factors.

3. Simulation results

To verify basic functionality of the model three basic scenarios were created. The paper deals only with an economic motivation for the capability pooling and sharing. Other parameters, such as trustworthiness, stability and sovereignty are behind the scope of the paper.

In all three scenarios we suppose the following values. Initial values of the capability at time $t_0 = 0 t_0 = 0$: $InitCAPCZ = 3 InitCAPCZ = 3$, $InitCAPAL = 0{,}5 InitCAPAL = 0{,}5$,

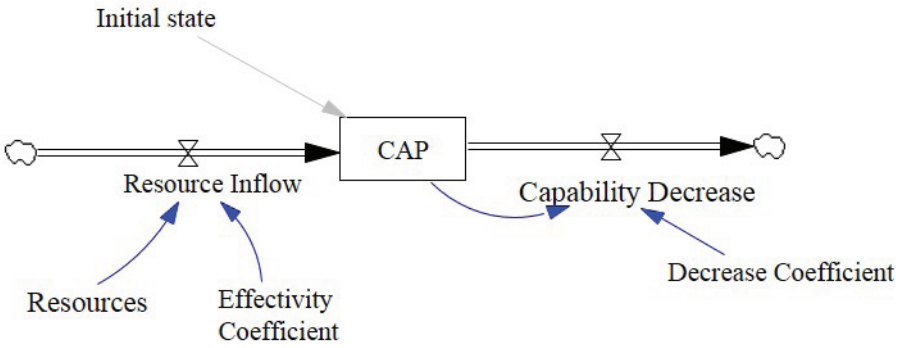


Figure No. 1 Capability stock and flow diagram

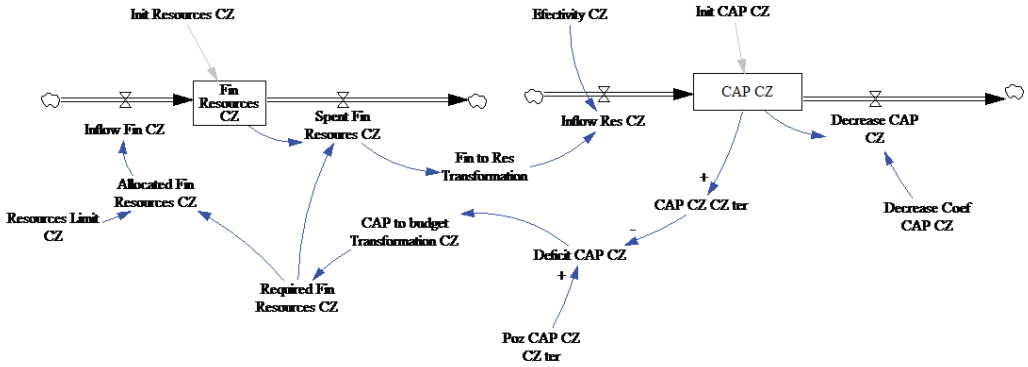


Figure No. 2 Dynamic model of capability building described by stock and flow diagram

$EffectivityCZ = 1 EffectivityCZ = 1$, $EffectivityAL = 0{,}6 EffectivityAL = 0{,}6$. Required capability values: $ReqCAPCZCZter = 5 ReqCAPCZCZter = 5$, $ReqCAPCZCZter = 2$ $ReqCAPCZCZter = 2$. Direct expenses of the capability sharing project are a supposed constant and equal to 0.1 [currency/month] on both sides. Time units are months, duration of simulations is set to 100 months.

Scenario S1 - smooth run. We suppose that capability sharing is driven by common economic interest, there is full trust between partners and the receiver (AL) has no sovereignty request concerning the capability$CAPCAP$. Financial resources are allocated according to needs, i.e. financial limits are not reached. The shapes of whole provider's capability $CAPCZCAPCZ$ and its distribution allocated to CZ and AL territories $CAPCZCZterCAPCZCZter$ and $CAPCZALter$ $CAPCZALter$ respectively are in

Figure No. 3 , for scenario S1 and for other two scenarios in

Figure No. 4 and

Figure No.5 respectively. Deficits in capabilities at provider's (CZ) and recipient's territories $DeficiencyCAPCZDeficiencyCAPCZ$ and $DeficiencyCAPALDeficiencyCAPAL$ for all

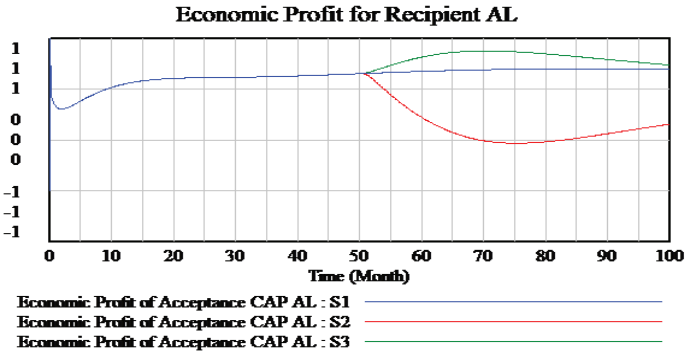
three scenarios are shown in

Figure No. 6. In this scenario (S1) the recipient gives up his own capability building and fully relies on the partner, driven by economic profit. The capability deficit converges to 0 due to fulfilled resource requests. In Figure No. 7 shapes of SharingPolicySharingPolicy for all three scenarios S1-S3 are drawn for comparison.

In other two scenarios, the step change in available financial resources occurs at time $t = 50t_z = 50t_z = 50$,[16] which is given by resources limit either for the capability provider (scenario S2), or for the capability recipient (scenario S3).

Scenario S2 – budgetary constraints for the provider. We assume that budgetary restrictions occur (at time $t_z = 50t_z = 50$) at the provider, which makes it impossible to achieve the required capability. However, the ability to share an economic interest persists; the capability is provided in accordance with the sharing policy. It is seen, Figure No. , that economic profit decreases to negative figures in case of the application of the sharing policy (4). Even if the value of this variable is rising later on and the continuation of the project is economically advantageous, the sudden reduction in the budget for the capability provider leads to a destabilization of the entire project, taking into account trustworthiness decrease, which would occur. In real life, it would be necessary to change sharing policy or to compensate for the recipient loss in another way.

*Scenario S3 – budgetary constraints for the recipient***.** In this case we suppose that budgetary restrictions occur at the provider side (at time $t_z = 50t_z = 50$), which makes it impossible to achieve the required capability. Economic profit for the recipient even rises due to the applied sharing policy, where earlier recipient's contributions into provider's capability $CAPCZCAPCZ$ are considered, see Figure No. 8. On the other hand, economic profit for the provider decreases because it is directly proportional to the shared capability, see Figure No. 9.



In case of too high direct expenses the provider's economic profit can be so low that the provider can terminate his participation in the project, which would probably result in a higher security risk (due to capability deficit) or in higher expenses later on (due to necessity of building own capability) at the recipient side, compared to the case of the stable budgeting of the shared capability.

16 The time of step change was chosen in the middle of simulation interval, when all values are stabilized after system initialization

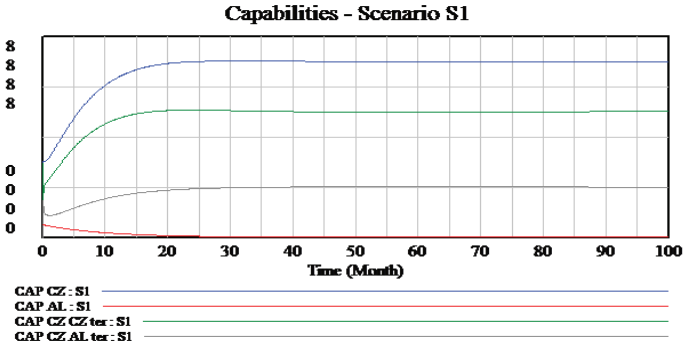


Figure No. 3 Capability and its distribution between partners – Scenario S1

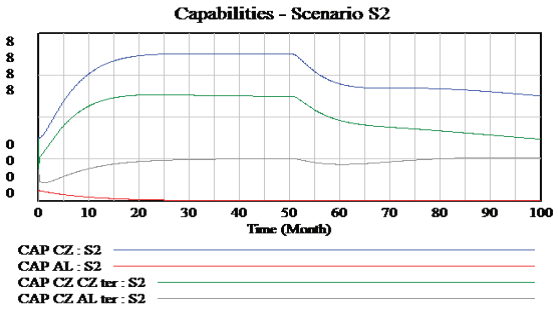


Figure No. 4 Capability and its distribution between partners – Scenario S2

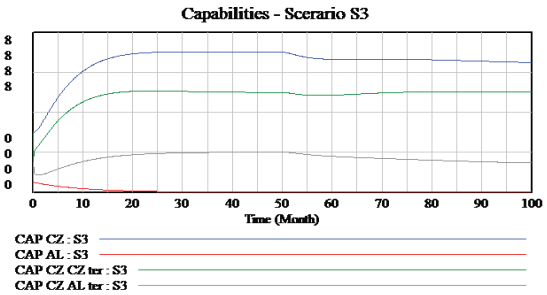


Figure No.5 Capability and its distribution between partners – Scenario S3

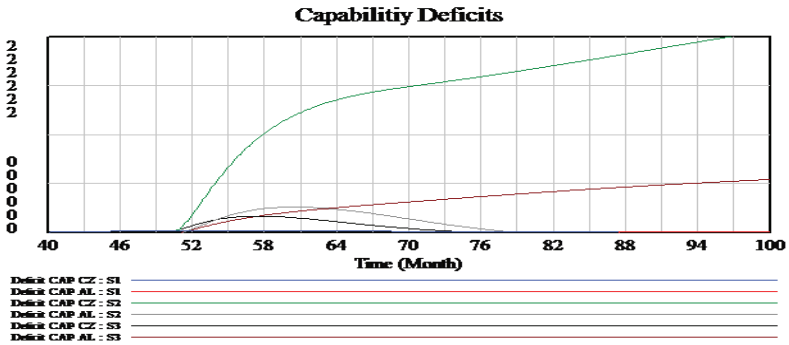


Figure No. 6 Capability deficits

Figure No. 7 Sharing Policies

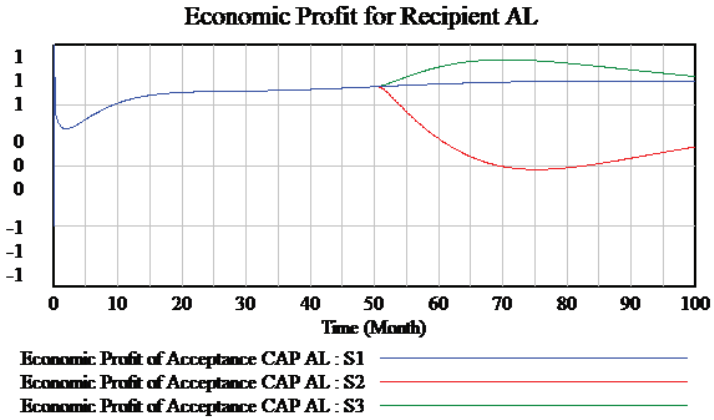


Figure No. 8 Economic Profit for Recipient

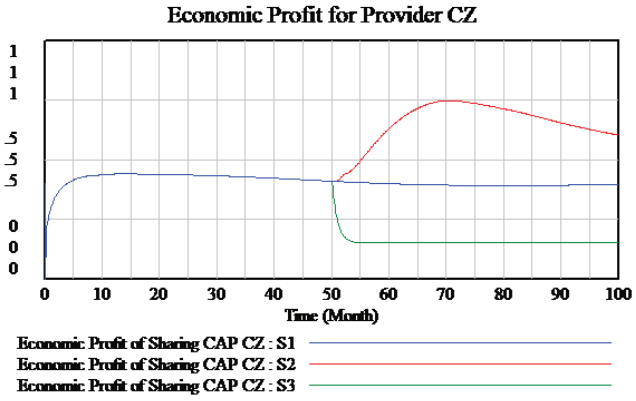


Figure No. 9 Economic Profit for Provider

Conclusions

Ambiguity of the Russian Federation behaviour in relation to Ukraine requires more than ever a strong solidarity between NATO members because only then credibility of the Alliance can be built. This solidarity implies in particular the active involvement of Member States in the process of building defence capabilities, especially those technologically advanced and very costly, which are often critical to the conduct of operations. This parameter is also already taken into account and applied by setting goals for NATO's defence planning - called "Principle 50%"

The article describes the application of methods of system dynamics to the process of sharing of military capabilities, the appropriate application methods of system dynamics modelling and simulation can help to assess the effectiveness and efficiency of involvement in the project of sharing military capabilities. The discussed ability model represents only the qualitative behaviour of the system. Its core consists of a simplified model of general capability and has deliberately disregarded quantitative parameters, nonlinearity building process capability (effectiveness varies with the level of capability attained), its components, and more. On the basis of the described basic scenarios it can be concluded that the model has met expectations and provides logically interpretable outputs. The model allows designing a mechanism to verify capacity building; equally important is the ability to share specific policies by individual participants.

The scenarios discussed in the paper provide a basic picture of the system behaviour. We can state that the system is stable (it converges to equilibrium state) and its behaviour fits our expectation, i.e. a capability drops corresponding changed resource limits. The presented dynamic model of the capability sharing process will be extended in a follow-on work. The dynamic model of capability building, which is a cardinal subsystem and can be dealt as a stand-alone model, requires further refining. Another direction for follow-on research is further analysis and specification of couplings among "soft" variables, such as trustworthiness, sovereignty, political will and stability (in a political sense), which are represented in a very simplified form in the presented model.

In order to apply this methodology to the specific capacity, quantification of the most important parameters is required. The model worked with only two parties, the provider and the recipient capabilities. Generalization of the project, which will contribute to more participants, can then be an analogous procedure. Sharing capabilities can be created as "belonging" to one entity or as collective sharing capabilities (e.g. AWACS), but the underlying mechanisms for building, sharing and dissemination capabilities will be the same.

BIBLIOGRAPHY:

1. MoD. Defence strategy of the Czech Republic. Prague, December 2012. Accessed on 2015-03-10. ISBN 978-80-7278-606-0. Available at web address: http://www.army.cz/images/id_8001_9000/8503/STRATEGIE_an.pdf
2. NATO HQ. Connected Forces Initiative. Brussels, September 2014. Accessed on 2015-03-10. Available at web address: http://www.nato.int/cps/ en/natohq/topics_98527.htm
3. NATO HQ. Improving NATO´s capabilities. Brussels, February 2015. Accessed on 2015-03-10. Available at web address: http://www.nato.int/cps/en/natohq/topics_49137.htm?selectedLocale=en
4. NATO HQ. Multinational Projects. Brussels, June 2014. Accessed on 2015-03-10. Available at web address: http://www.nato.int/nato_static_fl2014/assets/

pdf/pdf_2014_06/20140602_140602-Media-Backgrounder_Multinational Projects_en.pdf
5. NATO HQ. Multinational Projects. Brussels, November 2012. Accessed on 2015-03-10. Available at web address: http://www.nato.int/nato_static/assets/ pdf/ pdf_2012_10/20121008_media-backgrounder_Multinational-Projects_en.pdf
6. NATO HQ. Press Release. Wales summit Declaration. Brussels, September 2014. Accessed on 2015-03-10. Available at web address: http://www.nato.int/cps/ en/ natohq/official_texts_112964.htm
7. NATO HQ. Summit declaration on Defence Capabilities: Toward NATO Forces 2020. Brussels, May 2012. Accessed on 2015-03-10. Available at web address: http://www.nato.int/cps/en/natohq/official_texts_87594.htm?mode=pressrelease
8. Pruyt, E. Small System Dynamics Models for Big Issues: Triple Jump towards Real-World Complexity. Delft, TU Delft Library 2013. ISBN: 978-94-6186-195-5.
9. Statement NATO SG A. Fogh Rasmussen before NATO summit in Wales. Accessed on 2015-03-10. Available at web address: http://www.theguardian.com/ world/ video/2014/sep/04/nato-summit-newport-most-important-in-alliance-history-video
10. STEJSKAL, Jan. NATO Defence Planning Process in (Permanent) Transition. Prague, 2013. Czech Military Review, Volume 22 (54), No. 3, pp. 71-80. ISSN 1210-3292. Accessed on 2015-03-10. Available at web address: http://www.vojenskerozhledy.cz/kategorie/obranne-planovani-nato-neustale-v-tranzici?highlight=WyJzdGVqc2thbCJd

CHALLENGES FOR DEFENCE PLANNING – BUSINESS PROCESS OPTIMISATION AND PERFORMANCE MANAGEMENT

Josef PROCHÁZKA, PhD
LtC (Ret), Eng., Deputy Director of the Centre for Security and Military Strategic Studies - University of Defence, Kounicova 65, 662 10 Brno, Czech Republic,
e-mail: josef.prochazka@unob.cz

Abstract: *The article identifies some of the most significant challenges related to the implementation of a modern defence planning system as the most important business process of defence organisation and to the introduction of a performance measurement framework in non-profit organization in general and in defence sector particular. It offers possible ways to address those challenges. Main challenge in this endeavour is the ability of defence planners to set up measurable and manageable objectives (smart objectives) across the defence organization which would offer the strategic level management the nearly real time situational awareness about the MoD´s corporate strategy implementation and allow realistic assessment of defence sector performance. Additionally, it would also support transparent allocation of resources - chiefly for long-term investments.*

Keywords: *defence planning, performance measurement, SMART objectives*

Introduction

Since the end of ´80 almost all Central and Eastern European Countries (CEEC) including the Czech Republic have undergone considerable structural defence reforms. The objective was to adapt their defence sectors to the new security and social landscape. In this endeavor robust military capabilities designed for the purpose of a geostrategic bipolar confrontation have disappeared. They were offset by smaller mostly professional Armed Forces transformed for the challenges of 21st Century - expeditionary kind of warfare and confrontation with asymmetric opponent.

Armed Forces transformation of the CEES has encompassed both military capabilities and defence sector management. In the course of reforms best practices in strategic defence management derived from modern western democracies have been examined and in some extend also implemented. Defence sector management reforms[1] have mostly aimed at ensuring supremacy of politics over military and introducing credible strategic management framework with a strong planning function interlinked with defence resource management (finance, human and property) and armament. The overall objective was to strengthen effectiveness and efficiency of all business processes and enhance functioning of defence sector. Despite significant progress and tangible outcomes in many areas there is still enough space for further improvement. One of the most promising areas is the strengthening of planning function and introduction of performance measurement in military (non-profit)

[1] Main elements of strategic defence management: defence policy formulation, defence planning, defence resource management (finance, personnel, property) and armament. In: Bucur-Marcu H., Fluri P., Tagarev T., *Defence Management: An Introduction.* Security and Defence Management Series no.1. Geneva : Geneva Centra for the Democratic Control of Armed Foces, 2009. ISBN 978-92-9222-089-1

organizations. This requirement has been underscored by ever shrinking defence budgets of almost all CEES as their governments have responded to the prolonged economic crisis.[2]

Before 1999 planning function within Czech´s MoD was restrained mainly to the short-term horizon. More importance has yield the budget preparation and its execution. This situation had a negative impact on an effective functioning of the entire defence sector. Most importantly there was disconnect between rather short – term political cycle in the Czech Republic[3] and decision making process embracing a long-term investment in equipment, infrastructure and people. After the Czech Republic joined NATO in 1999 the MoD has strived to establish modern defence planning framework as a main component of defence sector strategic management.

In the meantime, the MoD has significantly enhanced its planning ability. Defence planning process focuses on a holistic approach to capability development applying functional areas according to NATO DOTMLPFI[4] methodology. It also harmonizes defence planning with defence resource management through the common set of objectives. In addition it institutionalizes short- and mid-term planning horizon. However, some deficiencies still persist e.g. the objectives formulation and description lays far away from SMART approach, planning still missies long-term horizon and the linkage to the acquisition process is insufficient in order to create precondition for timely, on budget and within scope capability delivery.

In recent years more emphasis in public non-profit organizations has been put on the output rather than input, as a result of growing pressure due to the ever shrinking public budgets. In order to address this requirement and seek higher level of effectiveness and efficiency an initiative to implement objective-based planning and budgeting was introduced by the Czech´s MoD. Nevertheless, this approach, so far, struggles with little interest of the MoD top management. This is partly due to the relatively substantial administrative burden and rather limited value added to the strategic management daily routine.

1. Planning as a core strategic management function

There was a sort of skepticism about the usefulness of a systematic planning after the political and social change in the Czech Republic in 1989 (at that time in Czechoslovakia). The consequent abolishment of central planning capacity within the state administration underscored this evolving posture and led to the introduction of so called management by money. Although the market economy was rightly seen as the most powerful instrument to guide the demand and its satisfaction the non-profit public domain found itself in a vacuum. In the case of defence, the defence budget and short-term planning became the only tools to manage the defence sector. This situation had a negative impact on the development and daily operations of entire defence sector because its nature - e.g. the level of complexity, a long-life

---

[2] The financial crisis has negatively affected Czech´s government finance. Due to the slump, the government deficit raised from 2.7 per cent of GDP in Fiscal Year (FY) 2008 to 5.8 per cent in FY 2009, and subsequently the government debt increased from 30 per cent GDP in FY 2008 to 35 per cent in FY 2009. According to Excessive Deficit Procedure, a set of across-the-board austerity measures had to be executed, in order to prevent an excessive deficit. There was a considerable drawdown in defence spending; the 2010 MoD budget dropped by more than seven billion CZK, in comparison with FY 2009, and the 2011 one was by five billion CZK lower, then the 2010 one. *The Czech White Paper on Defence 2011.*

[3] Since 1989 there were 16 ministers of defence appointed and more than 20 strategic and conceptual documents adopted by the Czech´s Government. These facts underscore the political instability related to the defence policy formulation and its implementation. Available at: http://www.army.cz/scripts/detail.php?id=89972

[4] Assessment and detailed evaluation of required operational capabilities can be performed in following functional areas: Doctrine, Organisation, Training, Materiel, Leadership, Personnel, Facilities and Interoperability. *In: Czech´s Ministry of Defence Planning Directives 66/2012.*

cycle of military equipment and preparation of suitable personnel - requires a credible planning function spanning short -, mid- and long-term horizons.

While it might be seen impossible from the sceptics' point of view to predict the future, thinking about the future is essential for military organisations to formulate concepts, strategies, plans and initiatives that will be effective across the widest range of contingencies, and executable within projected resource limitations.

The existing gap in planning function causing billions of Czech Crowns being vested has become even more apparent when the Czech Republic started its accession dialog with NATO. Under this external pressure attempt has been made to adopt Planning, Programing and Budgeting System (PPBS) based on the US lessons learned. That initiative failed mostly due to different strategic culture in the Czech Republic and level of organizational maturity of its defence sector. Window of opportunity to improve planning process within the Czech MoD was opened again with the NATO membership (*12MAR1999*). New set of so called defence laws was adopted by the Czech Parliament in 1999. This step created necessary legal framework for more conceptual approach to the development of defence sector and the Czech Armed Forces (CAF). It also resulted in the elaboration of the CAF vision and strategy.[5] In order to support this positive trend defence planning function in the Czech MoD has been a subject of further improvement.

First of all, defence planning was designed as a capability driven process ensuring a complex development of the CAF and its relevance for the future type of military confrontations. Rather functional approach to defence planning and capability development was implemented. The NATO DOTMLPFI methodology was used as one of potential tools to support a holistic approach to capability development.

Secondly, defence planning was oriented on outputs. It means that defence planners priority number one is the definition of desired end state and identification of effects which military organization should achieve. Less effort should be spend on incremental style of planning and budgeting preserving old strategies, trends, behavior and adaptation restraining culture. This approach has also a potential to contribute to the development of the CAF responsive to future challenges and enhancing probability of its usefulness in future wars.

Thirdly, defence planning is to provide real time situational awareness for the strategic management on its strategy implementation (measurement of success – performance measurement). Consolidated kind of strategic level feedback must also provide required level of transparency for all stakeholders including the taxpayers. Additionally, it should allow for clear accountability in case that a deviation from originally approved plans is identified. Furthermore, corrective actions might be sought and implemented.

Finally, based on the above mentioned argumentation there is a need for a systematic process to formulate and implement mission, vision, strategy, plans and initiatives in defence sector strategic management and obtain realistic and timely manner feedback about it. The answer might be a strengthened credible planning function with an appropriate performance management framework.

2. Performance management – necessity or administrative exercise

In general, performance management is a set of management and analytical processes that enable the managers to formulate objectives, put in place key performance indicators (KPIs) in order to monitor their implementation, assess progress and take appropriate

[5] Concept Development of Professional Armed Forces and Mobilisation of the Czech Republic Defence Forces. Adopted by the Government of the Czech Republic Nov. 2002. Available at: http://www.army.cz/scripts/detail.php?id=1572

correction and mitigation measures if required. Performance management activities in large organizations - as the MoD definitely belongs to – also involve the collection and reporting of large volumes of data. Although performance management is often incorrectly understood as an activity that necessarily relies on software systems to work, it is a challenge for any given organization to provide consolidated, reliable and relevant data in timely manner for comprehensive strategic overview about organization´s state of matters.

Performance management builds on a set of concepts and methods to improve decision-making by using fact-based support systems. The strategic defence management requires extracting useful information and turning that information into actionable knowledge. The performance management framework gives organizations a top-down framework by which to align planning and execution, strategy and tactics, and strategic level objectives with tactical level tasks.

In the case of the Czech MoD a three-level-objectives is maintained. It creates a common framework both for planning purposes and budgeting. First two levels of strategic objectives are stipulated in the Defence Minister´s Guidance. This document informs the planning cycle on yearly basis and is approved by the Defence Minister by March each year. Set of strategic objectives is being formulated in accordance with the Czech´s national law, strategic documents (Security and Defence Strategy), Czech´s commitments towards international organization primarily NATO and EU e.g. the commitments towards the fulfillment of capability targets accepted by the Czech Republic during the negotiations in the framework of the NATO Defence Planning Process.

These two levels of strategic objectives are being further elaborated by top level managers within the MoD structure in to the third rather operational level of objectives. This process is to ensure that there is a clear understanding of the ownership and accountability for each objective. Set of objectives serves as the basis for mid-term and short-term planning. Specific measures are designed to fulfill the objectives and prioritized against the available resources taking in consideration operational risks. Figure 1 depicts the main elements of the Czech MoD planning process while applying the management by objectives.

Although it looks like that the Czech MoD planning process is designed in order to measure performance of the entire defence sector, yet, several deficiencies still persist and limit the potential for effectiveness and efficiency which this approach actually offers.

The Czech White Paper on Defence 2011 stipulates clearly that the contemporary managerial approach is still focused rather on inputs. A shift from the traditional cash-based to an accrual-based accounting and budgeting is needed in order to enhance economy, efficiency, and effectiveness of utilization of inputs within armed forces. The heart of the matter lies in an insufficient linkage of resource management process to mid- and long-term planning information on achieved results, especially how they correspond with the formulated targets and their indicators, is not available either.

Figure 1: Czech MoD planning process – objectives hierarchy and documents[6]

There are several findings from the latest performance management framework assessment. First of all, the objectives hierarchy is a combination of the Czech MoD organizational structure and its functional interdependences (see figure 2). This approach does not lead to the necessary sort of harmonization of activities and effort among the MoD elements towards the fulfillment of its mission and strategy. In some extend it is the outcome of an organizational culture and mindset that constrains the effective use of project management and creation of project oriented organizational structure (integrated projects teams). Managers are not prepared and processes are not designed in order to balance responsibility for the fulfillment of across-organizational objectives and accountability for use of resources.

Secondly, managers on all levels are not properly involved in the objectives formulation and identification of key performance indicators (KPIs). They still consider this process administratively too heavy with only limited value added to their day-to-day managerial routine. Under these circumstances the responsibility for objectives formulation and identification of KPIs rests mostly with the defence planners' community. Managers - even responsible for planning - get in many distances involved too late in process, mostly in the moment that things are being already implemented and they have to made decisions on resource allocations. It is one of the reasons that the Czech defence budget execution is a subject of permanent change – budget execution looks differently from the mid-term plan deliberations.

[6] The design of the author.

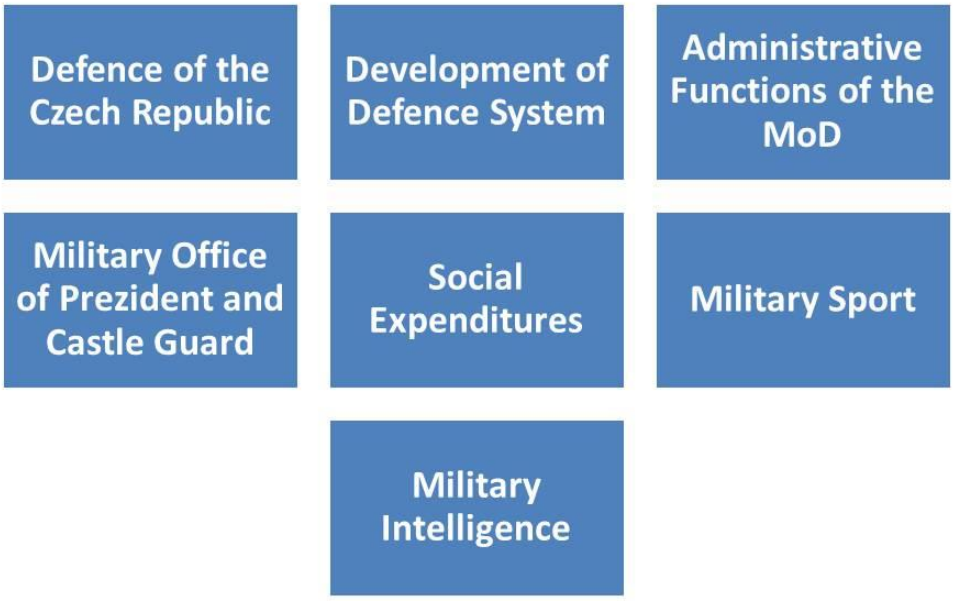


Figure 2: Czech MoD Strategic Objectives – Level 1 as of as 2012[7]

Thirdly, defence planners still struggle to formulate SMART objectives and KPIs which would allow for monitoring of performance and the Czech´s MoD strategy.[8] The formulation of political and military end state is rather vague and KPIs do not measure real effects of performed activities. KPIs provide rather information about fulfillment of those activities as e.g. number of exercises and workshops or elaboration of different sort of documents. Nevertheless, effort continues to improve skills of planning community by specifically designed course and lessons are being learned on regular basis with the accomplishment of each planning cycle.

Furthermore, the reporting cycle based on quarterly reporting on budget execution and semiannual reporting on the annual plan implementation is far away from the real-time situational awareness on strategy implementation.[9] In order to improve this rather unsatisfactory state of play consolidated data relevant to the KPIs must be provided on the near-real-time basis through the information systems supporting almost all business process in the Czech MoD.

Finally, in the planning process, clearly formulated objectives enable the MOD to defend its entitlements to financial resources against the executive and legislative bodies of

---

[7] *Resource: The Czech White Paper on Defence 2011. Available at: http://www.mocr.army.cz/informacni-servis/zpravodajstvi/plne-zneni-bile-knihy-o-obrane-55515/*

[8] In the framework of the planning process, objectives are further defined into specific measures and tasks. The methods of their attainment must be clear, i.e. they must specify personal responsibility, deadlines, resources, costs and required quality. This is also a precondition for monitoring the process of achieving the objectives. *The Czech White Paper on Defence 2011.*

[9] The Czech MoD strives to reach a maximum level of transparency and clarity of its defence policy. For this reason, it submits the Report on the Czech Republic Defence to the Government on a yearly basis. This report evaluates the state of defence, shows deficiencies in capabilities, analyses their causes, suggests corrective measures, and identifies risks. The main conclusions and recommendations of this report are available to the public. *The Czech White Paper on Defence 2011.*

the Czech Republic. At the same time, such a system ensures transparency of public control over the use of public funds allocated to defence. The current financial management enables to grant funds for all organizational elements of armed forces and to fund them, but its ability to enforce economy, efficiency, and effectiveness of their use is rather disputable.

3. Balanced scorecard is more than a monitoring strategy implementation

Since 1992, performance management has been strongly influenced by the rise of the balanced scorecard (BSC) methodology. This methodology offers a framework to clarify the objectives of an organization, to identify how to track them, and to structure the mechanisms by which interventions will be triggered. These steps are the same as those that are found in performance management processes.

The catalysts for BSC application were two major deficiencies. The measurement gap (performance measures not integrated into the strategy formulation process) and the performance gap (lack of rigorous integration between strategic level (corporate) direction, short-term actions and activities and performance measurement). Managers have to seek to drive strategy down and across their organizations, transform these strategies into actionable metrics and use analytics to expose the cause-and-effect relationships that, if understood, could give insight into decision-making. The BSC can facilitate this effort.

The BSC has been studied in a variety of non-profit environments where a balanced set of measures is tied to different points of focus within an organization that are more commonly categorized as: learning and growth capabilities, the efficiency of internal processes, customer value, and financial success. The 1st generation-BSC measures performance from these four perspectives and provides more coherent strategic picture about an organization's performance but it was focused more on strategy and vision and less on the way BSC is designed. The 2nd generation-BSC goes further. It uses a casual "strategy map" to define strategic objectives and to identify activities and results that need to be measured. In the late 1990s, the design approach had evolved yet again. One problem with the "second generation" design approach described above was that the plotting of causal links amongst twenty or so medium-term strategic goals was still a relatively abstract activity. In practice it ignored the fact that opportunities to intervene, to influence strategic goals are, and need to be, anchored in current and real management activity. Secondly, the need to "roll forward" and test the impact of these goals necessitated the creation of an additional design instrument: the Vision or Destination Statement. This device was a statement of what "strategic success", or the "strategic end-state", looked like. It was quickly realized that if a Destination Statement was created at the beginning of the design process, then it was easier to select strategic activity and outcome objectives to respond to it. Measures and targets could then be selected to track the achievement of these objectives.

There´s no reason an organization must use exactly the same set of perspectives – each entity can develop its own dimensions of importance. The goal of this contribution is to get you think beyond the familiar scorecard design for a for-profit organization. Whether public or private, profit-oriented or non-for-profit, all organizations must invest in learning and growth in order to improve their internal processes, people, facilities and technology. For military kind of organization, however, the key perspective is readiness. Readiness is about providing combat ready military capability for execution of operations and missions when called on – main component here is the training – the ability to act in crisis respond operations and wars.

Military capability might be understood as the ability to achieve a desired effect in a specific, operating environment.[10] Military capability is composed by several interdependent factors taking in the consideration the DOTMLPFI methodology. In this regard developing objectives into measures and tasks must be a complex activity that includes qualitative as well as quantitative aspects and criteria, such as doctrinal directives, optimizing organizational structures, adjusting training and education, supplying material, leadership and personnel management, defining requirements for personnel skills and abilities, infrastructure, interoperability and international cooperation.

The most advanced performance measurement framework should fulfill the following attributes:

- *Simplicity.* Framework should consist of from 10 – 20 metrics.
- *Explicit links to strategy.* KPIs should be tightly coupled to the strategic planning process and assist in tracking progress against key goals and objectives.
- *Broad executive commitment.* Defence political leadership and senior managers should be involved in the process of formulation of strategic direction, creating performance measurement framework and ongoing monitoring of success.
- *Consensus.* Consensus should be achieved on KPIs definitions.
- *Unity of effort.* KPIs should interlink strategy with tactical level activities and allow for detailed review of trends by providing more granularity on component elements.
- *Accountability.* Individual manager´s responsibilities and evaluation should be linked to performance.

Based on own analysis the possible design of performance measurement framework in defence sector may track objectives and KPIs in following perspectives: (1) operational; (2) readiness; (3) financial; (4) modernization; (5) optimization; and (6) human resource.

You can find proposed set of objectives related to each perspective below.

1. Operational Perspective
- Crisis response operations and missions
- Defence of the Alliance Air space
- Contribution to NATO and EU rapid reaction forces

2. Readiness Perspective
- Provision and sustainment of credible defence (manned and equipped structure and infrastructure)
- Training (certification of units and readiness assessment, support)
- Deployment of defence force

3. Financial Perspective
- Financial performance (including risk assessment and cost-benefit assessment)
- Balanced Defence Budget structure (Personnel Expenditure, O&M, Investments)
- Contribution to collective defence

4. Modernization Perspective
- Deliver capabilities on time, on budget and within the agreed scope
- Multinational cooperation in capability development
- R&D, innovation and creative solutions

5. Optimization Perspective
- Adaptation of business processes

---

[10] Hinge, Alan (2000) *Australian Defence Preparedness: Principles, Problems and Prospects : Introducing Repertoire of Missions (ROMINS) a Practical Path to Australian Defence Preparedness*, Australian Defence Studies Centre, Canberra.

- IT Support (harmonization, resilience)

6. Human Resource Perspective
- Learning and Knowledge management
- Employees' Motivation
- Career Management (evaluation, promotion, laying off)

This approach provides holistic view on defence sector. It reflects its mission (purpose of existence), core business (main roles) and necessary supporting functions. It might also orchestrate effort of all personnel to support its mission. However, further effort is required to develop KPIs for each objective while reflecting the strategic defence management intent on speed of required change, realism on feasibility and acceptance of risks.

Conclusions

The article offers an insight into contemporary challenges of defence planning of the CEEC struggling with the legacy of their political and social system transition after the collapse of communist's regimes. This transition process has also significantly influenced both the defence management reforms and adaptation of their Armed Forces capabilities to the new reality. The already proved methodology and procedures offered by modern western allies have been examined and in some respect also implemented.

The case study of the Czech Republic stipulated in this article offers several lessons to be learned. A credible modern defence planning requires complexity (DOTMLPFI approach), long term focus, smart set of rather functional than organizational objectives elaborated into measures and initiatives to guide effort of all defence sector personnel. Furthermore, an effective management needs a realistic performance measurement framework consisting of achievable KPIs to allow for monitoring of desired end state (effects) and mitigating disproportions if required. Additionally, managers must be supported on the need-to-know basis by nearly-real time situational awareness with the consolidated data flow from available information systems of related internal business processes. Managers should understand the value added of modern performance oriented defence planning and budgeting for their daily managerial routine in order to support and get involved into all related processes.

In order to harmonize effort and coordinate activities across the defence sector the BSC methodology provides the useful framework not only for profit-oriented organizations but also for public sector. The possible way to address this issue is a modified BSC methodology. Its perspectives are designed to reflect defence sector core business – defence of country. In this regard emphasis is put on operational effectiveness, readiness and development of credible, sustainable and affordable capabilities.

BIBLIOGRAPHY:

1. The White Paper on Defence approved by the Governmental Resolution Nr. 369, as of May 18 th, 2011. The Ministry of Defence of The Czech Republic 2011. Available at: http://www.army.cz/ministry-of-defence/newsroom/news/the-white-paper-on-defence-2011--63155/
2. Albright T., Gerber Ch., Juras P. How Naval Aviation Uses the Balanced Scorecard. Strategic Finance, October 2014. p.21-28. Available at: http://www.imanet.org/ docs/default-source/sf/10_2014_juras-pdf.pdf?sfvrsn=0

3. Kaplan, R.s. and Norton, D.P. (1996) *The Balance Scorecard – Translating Strategy into Action* (Boston, MA : Harvard Business School Press).
4. Kaplan, R.s. and Norton, D.P. (2001) *The Strategy Focused Organization* (Boston, MA : Harvard Business School Press).
5. Mojdeh S., *Technology-enabled Business Performance Management: Concept, Framework, and Technology*. 3rd International Management Conference. pp. 1–9. Available at: http://www.mbaforum.ir/download/335_Full_sanamojdeh.pdf
6. vom Brocke, J. & Rosemann, M. (2010), Handbook on Business Process Management: Strategic Alignment, Governance, People and Culture (International Handbooks on Information Systems). Berlin: Springer
7. White, Colin The Next Generation of Business Intelligence: Operational BI. *Information Management Magazine*, 2005.
8. Dresner H. (2007) The Performance Management Revolution: Business Results Through Insight and Action. ISBN 978-0-470-12483-3.
9. Cokins, G. (2009) Performance Management: Integrating Strategy Execution, Methodologies, Risk, and Analytics. ISBN 978-0-470-44998-1
10. Paladino B. Five (2007) Key Principles of Corporate Performance Management. ISBN 978-0-470-00991-8
11. Wade D., Ronald R. (2001) Corporate Performance Management. Butterworth-Heinemann, ISBN 0-87719-386-X

THE AUTHORITY OF MILITARY ADMINISTRATION. THE RIGHT TO COMMAND IN THE ARCHITECTURE OF MILITARY ADMINISTRATION

Marian Paul FUSEA
PhD student in Military Science, National Defense University "Carol I"
Bucharest, Romania, e-mail: fuseapaul@gmail.com

Abstract: *Theoretical boundaries in the conceptual spectrum of the military authority. The military authority understood as a formal significance of the military administration's "power" to command. The military authority – special area of the public authority. The main normative acts regarding the structure and the application of the military authority. Delegated authority and transferred authority – procedures of ensuring the continuity of the military authority in the international or national military administrations*

Keywords: *administration, military authority, authority delegation, authority transfer*

Introduction

The theoretical research of the matters regarding the *military administration*, a complex field in the systemic space of the social construction, cannot avoid the discussion of its authority, as a fundamental vector of the accomplishment of the missions that are constitutionally assigned, as well as those derived from it, the missions of the military administration, being the imperative "pretext" of the definition of the *institutional authority* of the *military administration*. To understand the institutional and the operational signification of the *military authority administration*, we will focus on the concept that determines and represents it, respectively the *military administration*. In the systemic dimension of the society, the *military administration* is a subsystem of the public administration, and equally, a subsystem component of the global social system, meaning by this the social system defined by its national and state coordinates. *Stricto sensu*, the conceptual model discussed in the specialty papers, give the *military administration* definitions that either describe it as "*all the activities regarding the organization, equipping, material and financial providing for the armed forces, as well as the development of the of the specific rules for applying in the army the state legislation and normative acts*"[1], either as a set of actions whose purpose target "*organization and management by the military authorities of the whole activity performed on enemy soil occupied in time of war or as a consequence of it.*"[2] Admitting both components of the definition, as inseparable parts of the concept and taking into consideration the systemic relations between the social system, the public administration and the military administration, we can accept the following definition of the *military administration*: "*the activity of organizing the execution and enforcement of the laws of the country in the military field through actions with dispositive or provider character*"[3], activity which "*is realized by the Ministry of Defense, as central body of the public administration, through its specialized bodies and the devolved structures and/or decentralized in the territory.*"[4]

[1] Military Lexicon, Sakura Publishing House, 1994, p.15
[2] *Ibidem,* p. 15.
[3] Eugen Bădălan, The military administration – Dissertation, The National School of Political Science and Public Administration, Public Administration Faculty, 2003, p.49
[4] *Ibidem,* p. 50.

1. The Military Authority

1.1 The military authority in the Romanian legislation

In the area of conceptual boundaries regarding the military administration, the basic feature of enforcing prerogatives within the military administration, in the applied state of its operational formula, *is the military authority*.

It is considered that the *military authority* is represented by the military administration's right to command, to give directives, in situations stipulated by law.

The digression, from the specific comprehension of *the military authority*, as it is found in the Romanian legislation, indicates exceptional situations, in which the military administration has de decisive role. Thus, searching for the references in the legislation to the military authority notion, we find it, firstly, in the law regarding the civil status, in which it is stipulated that in the documents for granting the citizenship, given that a territory is under the military administration jurisdiction, are presented: " … *extracts from the civil status documents which were issued by the military authorities under the law*"[5]. A more pronounced use of the phrase it is found in the Law[6] regulating activities specific to the military administration, specifying issues like: "*the goods are commandeered only based on the order issued by the military authorities*"[7]; "*The delivery order of the commandeered goods will compulsory include the nomination of the issuing military authority*, *and the beneficiary military unit, the legal base of the commandeering, identification data of the goods, of the owner or the possessor, as well as specifications of the place and the place and term of the delivery of the goods"*[8]*; "The commandeering order will compulsory include: the name of the issuing military authority***,** *and the beneficiary unit, the legal grounds of the request, the name, surname and the address of the requested person, the term and the location where to be presented"*[9]. In another normative act[10], regulating the military administration's activity in the term of the state of siege, quoting the military administration's role, there are specified it's legal rights, more important being the following: "*In exercising the attributions in their duty in the period of the state of siege or the state of emergency, the military authorities issue military commands having force of law (...)*[11] *... " the information regarding the state of siege or the state of emergency, excepting those referring to natural disasters, are published only with the notification of the military authorities"*[12] *... "The military commands are issued on the period of the state of siege by the minister of national defense or the Chief of General Staff, as exclusive military authorities at national level, when the state of siege was established on the entire territory of the country."*[13] *... "The military command includes (...) the issuing military authority, the legal grounds, the period of application the date, the stamp and the signature of the issuing authority"*[14] *... "On the period of the state of siege, (...) a) the application by the military authorities of the measures provided in the approved plans according to the provisions of the present emergency order and the decree of establishment, is compulsory."*[15]

Likewise, the defined role of the *military authority* is cited in the law regarding the *Agreement between the member states of the North Atlantic Treaty Organization and the*

---

[5] Law no. 119 from October 16th 1996, republished and actualized, regarding civil status documents, Official Monitor no. 339 from May 18th 2012.

[6] Law no. 132 from July 15th 1997, regarding the commandeering of goods and services in public interest, Official Monitor no. 161 from July 18th 1997.

[7] *Ibidem*, Art. 14, alin. (1).

[8] *Ibidem*, alin. (2).

[9] Ibidem, Art. 17, alin (2).

[10] The Govern Emergency Ordinance nr. 1/1999, regarding the conditions of state of siege, and the conditions of the state of emergency, The Official Monitor nr 22 from January 22nd 1999

[11] *Ibidem*, Art. 8

[12] *Ibidem*, Art 23, pct. "i"

[13] Ibidem, Art 23, alin. (1)

[14] *Ibidem*, Art 24. Lit. b,c,d,e,h

[15] *Ibidem*, Art 26, alin (1)

participant states to the Partnership for Peace[16]*,* in which are defined, especially the *military authorities* of the sending state, as well as the main attributes, stipulating: *the military authorities of the sending state are those authorities invested with command attributions and with attributions of applying the legislation of that state regarding the members of its force or the civilian component"*[17] *... "The sending state's military authorities will grant all the support to ensure that the goods susceptible to be seized by the Romanian custom or fiscal authorities or on their behalf will be made available for the respective authorities."*[18] *... "the sending state's military authorities will have the right to exercise the penal jurisdiction or the disciplinary competence conferred by the law of the sending state in relation to persons subject to that state's military laws"*[19] *... "the sending state's military authorities will have the right to exercise their exclusive jurisdiction on persons subject to that state's military laws for the offenses, including to its security, incriminated by the sending state's legislation, but not by the Romanian law."*[20]

The interwar localization of the operational concept relative to the *military authority*, as an efficient operational instrument of the military administration acts, is identified in the constitutional enactment of the *military power*, in which, in fact, it was appointed the public power of military nature of the state. Specific but also significant of that period, is the opinion that "*the military authority through which the public order and state security is done is the Commander besides which it exists a court (The military Commander of the Capital, the army commandments and certain division commandments). All these commanders exercise these powers either directly, either by delegating certain attributions, on the garrison commanders from the respective juridical circumscription."*[21]

Allowing certain preliminary conclusions regarding the operational concept of *military authority/ military authorities*, it can be affirmed that: in the present Romanian legislation, the collocation military authority/military authorities does not have a strong use, this being an effect of the sluggish change in the defense and security culture after December '89 from the communist mentality to the democratic evolution paradigm: lacking a definition to conceptually explain the collocation *military authority* or *military authorities,* some have comprehensively subordinated, with the same meaning, names of some military institutions with a very powerful and well known public image – The General Staff or the staffs of all the services (forces), the area military centers, the specific commandments; the late and somehow feeble affirmation in the specific juridical literature of the notion of *military authority*, can be explained also by the fact that, in the same semantic sense, the collocations "*military bodies*" and "*military staff*" were largely used, having assigned, subliminally, the meaning of military authorities. We record that, according to the operational defining of the military authority, this concept does not refer to the relations present inside the military body, or the military institution, but exclusively to the direct relations of the latter with the citizens or the public authorities.

Regarding the military specific legislation, but also the internal normative acts arising from it we encounter the collocation – military authority, in the Military disciplinary regulation, in the issue from the year 2000[22]. In the body of the Regulation, the topic regarding "*The military authority and the obligations arising from it*"[23], is treated separately, however, in its following normative development, there are more common the terms "commanders", "superiors",

---

[16] Law no. 61 from April 24th 2000, for the application of the Agreement between the member states of the North Atlantic Treaty Organization and the participant states to the Partnership for Peace, regarding the status of their forces, signed in Bruxelles at June 19th 1995, The Official Monitor no. 185 from April 28th 2000

[17] *Ibidem*, Art. 1, pct. 5

[18] *Ibidem*, Art. 29, alin. (2)

[19] *Ibidem*, Art. 38, alin (1), lit b)

[20] *Ibidem*, lit d)

[21] Paul NEGULESCU, Administrative law treaty, vol. I, p.521

[22] "R.G.-3, The military disciplinary regulation, approved by the Order of the minister of national defense no. M. 70/2000, with the subsequent modifications and completions. The order wasn't published in The Official Monitor of Romania, Part I, because it covered defense and national security topics

[23] *Ibidem*, Chapter II

"hierarchical chiefs", "military structures", "upper echelon", all being used subliminally with the meaning of *military authorities.* We find that, probably because of a breach in the process of elaboration, in the context of the definition of the misbehaviors[24] it is appreciated that "*the lack of respect for the commanders, superiors, equals or inferiors in rank ant for the authorities*"[25]. The wording as such leads indirectly towards the supposition that the authorities referred to are exclusively civilian. We appreciate that this is a hiatus of theoretical process of defining the *military authority*, the construction of this concept not being fulfilled in institutional paradigms.

However, the document that frequently uses the notion of *military authority*, in certain way establishing this concept in the profile literature, is the General regulation for conducting military actions[26]. Being systematically subscribed to the notion of *authority*, we can find the concept in phrases that target and regulate: the stipulation according to which "the *commander is the authority legally invested or assumed which exercise the act of command on the personnel of the subordinated structures, as well as on the temporarily subordinated personnel*"[27] … the provision according to which "*the command act includes the authority and the responsibility for the efficient use of the available resources and for planning the action, organizing, coordinating and the control of the forces in order to accomplish the missions"*[28] ... the organizational role of the deputy commander, defining it as "*the invested authority taking part to the act of command within the boundaries established by the commander"*[29], as well as the role of the chief of staff, as "*authority invested with exercising the act of command on the staff, he can make decisions regarding the entire base, only in the absence of the commander or his deputy"*[30]. Likewise, in the supporting section of the of the Regulation we find defined "*the legally assumed authority"* as "*the right to issue orders, which a military assumes according to normative acts in force, to hierarchy of ranks, positions and competences in the field"*[31]

There are committed to memory, in this advocacy, the rules in force of the military discipline[32]. The document assigns one distinctive sector to the *military authority*[33], which entitles the supposition that the references to institutional roles of the military hierarchy are dealt with having the conceptual support of the *military authority*. It is withhold as representative for this exposure the assertion according to which "*The commander/chief represents the military authority legally invested with responsibilities and rights for exercising the acct of command in a military structure"*[34]. In the spirit of a endemic conclusion, it can be assessed "*the military authorities as being public authorities invested by the law with the exercise of public power, which have attributions of command and of applying the military legislation in their area of responsibility in times of peace, crisis and war, exercising it under civilian control from the public constitutional authorities, by military bodies with unipersonal or collective character, in compliance with the rules and principles of the public law."*[35]

[24] *Ibidem*, Art. 44
[25] *Ibidem*
[26] A.N.-2, The general regulation for conducting military actions, Bucharest, Military Publishing House, 1998
[27] *Ibidem*, Art.3
[28] *Ibidem*, Art.4
[29] Ibidem
[30] *Ibidem*, Art.17
[31] *Ibidem*, The dictionary of terms and phrases
[32] The military discipline regulation approved by the Order of the minister of National Defense, M.64 from June 10th 2013, published in The Official Monitor no. 399 bis, July 3rd 2013
[33] *Ibidem*, Section 2
[34] *Ibidem*, Art .11, alin. (1)
[35] Ion DRAGOMAN, *The military authorities acts*, LUMINA LEX Publishing House, Bucharest, 2003, p.108

1.2 The authority transfer and the authority delegation

The approach of the *military authority* concept requires considering its operational legal substitutes, respectively, the *authority delegation* and the *authority transfer,* very important in exercising the administrative and commandment acts of the military administration. The concepts are recorded and defined, according to the manner they act in the operational space of the military administration. The *delegation of authority* is realized according to the general rules, through which, in certain situations provided by law, it is used exercise the specific attributions of the public offices, by persons, other than the one fulfilling the institutional holder of the position. In this respect, the military normative system[36] contains clear provisions, stating that according to the situation, "*The commander of the military unit, in exercising the act of command, can temporarily assign, through delegation of competences, part of his duties and responsibilities to subordinates"*[37]. The descriptive analysis of the commander's attributions[38], indicate that the regulated amount of those (32 responsibilities, defined and delimited through distinct phrases), only two are not be delegated, respectively, the responsibility of "*providing the operational capacity of the unit"*[39] and the obligation to "*inform the deputy/chief of staff with necessary data for taking over the command."*[40]

Regarding the *authority transfer*, this procedure is specific to the operational context in which it is engaged a multinational force. It is the manner in which, according to rules assumed in consensus, the unique military command of all the forces taking part to the mission is assured, regardless of the country of origin. This means that all but one of the participant national military forces admit being under the command of a foreign military. Also it means that the *transfer of authority* represents the manner to provide continuous and unitary, from the point of view of concept and all the participant forces, the leadership for the multinational force, in other words, of the organization and execution by the *multinational military administration* of the assigned missions. From the conceptual perspective of this topic, the leading body of the participant multinational forces at such a mission can be assimilated, from the prospect of the administrative and commandment acts whit which it is responsible, to the *multinational military administration*. Thus it results a fist feature of the *authority transfer*. If the *authority delegation* operates al all the levels of the military administration, the *authority transfer* consists of the full transition of operational leadership of the participant forces at the mission in the responsibility of military leaders, others than those belonging to the national structure. The *authority transfer* is a very well developed procedure, preceded by the assuming by the military administrations of the states participating in the multinational force, but also by the political decision-makers in the respective countries, by consensus, of the Rules of Engagement[41]. These are "*directives issued by the political/military authority, towards the military structures participating to the military operation in which there are specified the circumstances and the limits within which they can initiate or continue combat actions with the opposing forces"*[42]. Legally based, the exercise of the national political control over the military and the assumed understanding of the military necessity, the Rules of Engagement guarantee the *transfer of authority* the administrative and operational framework of the multinational forces, without malfunctions, stagnations or specific involutions.

The *authority transfer* has a series of features which personalizes is a specific procedure of the multinational military administration, significant being:

---

[36] The internal regulations in military units, approved by the Order M.92, from September 17th 2008, published in The Official Monitor no.815, from December 5th 2012

[37] *Ibidem*, Art. 40

[38] *Ibidem*, Art. 43

[39] *Ibidem*, Art. 43, lit. a)

[40] *Ibidem*, Art. 43, lit u)

[41] Cf. Joint doctrine for multinational operations, Bucharest, 2001, Art. 123, alin. (1)

[42] Lt-Col Ion PARGULESCU Col. (r.) prof. univ. dr. Lucian SANCILA, "*The command and control of the structures of forces from the Romanian army during participating to post conflict missions, in multinational context", Colocviu Strategic* magazine, no. 5/2009, p2

- The *authority transfer* is produced without altering the principle of the command unit, which determines the operational cohesion of the multinational forces, any national contingent, part of the multinational force, can receive orders and instructions exclusively from the commander of the force, also by utterly from the multinational military administration;
- The *authority transfer* doesn't affect the administrative and jurisdictional authority under which the commander of a national contingent acts, these being under the operational authority of the multinational military administration, remaining fully subordinated to the national authorities of the country of origin (it isn't a double subordination, the subordination to the national authorities avoiding the separation of responsibility towards the resources, order and discipline of the forces in command);
- The *authority transfer* gives the military authority a well defined juridical framework, in the administrative and commandment acts of the multinational military administration. While the organizational interior of the national contingent the participant forces are subject to national legislation, in the multinational forces these fulfill exactly the administrative and commandment acts of the organization and execution, and the accomplishment of the missions, in accordance with the standard documents and procedures of operating the multinational alliance or coalition.

Conclusions

The presented conceptual arguments, entitle the conclusion that the military authority, through its operational features, represents the decisional support of the military administration. Moreover, the authority of the military administration legally consists in the act of command, in fact in making use of it, as a method of accomplishing acts and deeds of administration and command.

Also, the digression of the military authority concept allows a set of conclusions, whose theoretical value is stated in the following:

- In the Romanian legal and regulatory background, the term military authority / military authorities doesn't have a cursive use, this having the sluggish effect of transforming too slowly the defense and security culture from the post-December 1989 model to the democratic evolution of the society;
- Failing to give a definition to the term *military authority*, or *military authorities*, there are a set of authorities that can be conceptually subsumed to the same meaning: the General Staff, the Staffs of Forces, the regional military centers or the specific commandments;
- The late affirmation in the legal literature of the *military authority* term, can be explained by the fact that in the same semantic meaning, have been widely used phrases like "military bodies" and "military personnel", attributing them, subliminally the quality of military authorities;
- According to the operational consecration of the *military authority*, this does not refer to the relations manifested inside the military body, but solely to the direct relationship of the military institution with the citizens or the public administration.

BIBLIOGRAPHY:

1. A.N.-2, The general regulation for conducting military actions, Bucharest, Military Publishing House, 1998
2. Bădălan, E., The military administration – Dissertation, The National School of Political Science and Public Administration, The Public Administration Faculty, 2003
3. Dragoman, I, *Military Authorities Acts*, LUMINA LEX Publishing House, Bucharest, 2003
4. Joint doctrine for multinational operations, Bucharest, 2001
5. Law no. 119 from October 16th 1996, republished and actualized, regarding civil status documents, Official Monitor no. 339 from May 18th 2012

6. Law no. 132 from July 15th 1997, regarding the commandeering of goods and services in public interest, Official Monitor no. 161 from July 18th 1997
7. Law no. 61 from April 24th 2000, for the application of the Agreement between the member states of the North Atlantic Treaty Organization and the participant states to the Partnership for Peace, regarding the status of their forces, signed in Bruxelles at June 19th 1995, The Official Monitor no. 185 from April 28th 2000
8. Lt-Col Pargulescu, I., Col. (r.) prof. univ. dr. Sancila, L., "*The command and control of the structures of forces from the Romanian army during participating to post conflict missions, in multinational context", Colocviu Strategic* magazine, no. 5/2009
9. Negulescu, P., *Administrative law*, vol. I, II, 4th Edition, Graphical Arts Institute, Bucharest, 1934
10. R.G.-3, The military disciplinary regulation, approved by the Order of the minister of national defense no. M. 70/2000, with the subsequent modifications and completions. The order wasn't published in The Official Monitor of Romania, Part I, because it covered defense and national security topics
11. The Govern Emergency Ordinance nr. 1/1999, regarding the conditions of state of siege, and the conditions of the state of emergency, The Official Monitor nr 22 from January 22nd 1999
12. The internal regulations in military units, approved by the Order M.92, from September 17th 2008, published in The Official Monitor no.815, from December 5th 2012
13. The military discipline regulation approved by the Order of the minister of National Defense, M.64 from June 10th 2013, published in The Official Monitor no. 399 bis, July 3rd 2013

THE DECISIONAL SUPPORT FOR THE MILITARY ADMINISTRATION

Marian Paul FUSEA
PhD student in Military Science, National Defense University "Carol I"
Bucharest, Romania
fuseapaul@gmail.com

Abstract: *Theoretical engagement of the conceptual boundaries regarding the military authority, the military administration, commander, military bodies, military personnel. The decision-making, top responsibility of the military authorities. The decisional connection between the military administration and the military authority. The role of the military authorities in the planning, realization and the maximization of the military administration's decision. The command – attribute of the military authority. The significance of the order as an act of the military authority. Legal grounds of the military authority and decision.*

Key Words: military administration, war, central bodies, deconcentrated bodies, military structures

1. Introduction

Issues relative to the *military administration*, with the complementarities that maximizes its operationalization – the military authority administrative and command acts, were from the very beginning in the attention of the legal system, but also between the concerns of the decision makers of the national defense system. The attention granted to the military administration highlights both its importance in the national public administration system, and the imperative necessity for this part of the central administration system to have a rigorous legal validation from the legislative perspective. From this point of view, this presentation will be focused on highlighting the evolution of the concept of military administration, as well as its decision making support, ending by revealing operational interdependences between public authorities, the public administration and the military administration.

2. Developments in the conceptual background of the military administration

A retrospection of the Romania military reality, directed to the nodal periods of its evolution, depicts the military institution, at the moment of the formation of the Romanian state in 1859, as a professional body, organizationally connected, from the conceptual and training philosophy perspective, to the most advanced methods, principles and procedures of the time.

Considering the importance given to the discipline, in the process of establishment and maintenance of an active, competitive and coherent organizational condition of the military administration, not surprisingly, one of the first documents, unique in its extensive nature, was *Condica Penela Ostaseasca*[1] entered into force in 1860, replaced and developed, in 1873, by a similar document – *Codex of military Justice* which regulated the disciplinary conduct of the military administration until 1937.

The attention granted to strengthen the military administration is reflected by the continuous improvement of the particular nature criminal law, relevant being in this respect,

[1] "Monitorul Oastei" no. 13, from 1873.

the *Code of Military Justice*[2], document whose appearance was imposed by the legal resettlement of the Romanian state on the grounds and coordinates of the Criminal Code "Carol II"[3], act came into force in 1936[4]. The document conferred lawfulness to the administrative and commandment acts of the military administration. Also the document gave the military administration the legal framework for organizing and accomplishing the attributions and the specific missions.

After the collapse of the territorial structure that defined the National Unitary Romanian State, the normative reevaluation of the military juridical system, in which there had to be identified the new coordinates of the military administration, in the context of a different central government system, was mandatory. Given the circumstances, on July 31st 1940[5], the Code of Military Justice suffered significant changes and later it became the *Military Justice Code* "Mihai I"[6].

The legislative and regulatory perspectives conceptually attached to our topic – the military administration, reveal a continuous concern of the institutional factors to publicly maximize the military administration. The following examples are relevant.

The firs unambiguous mention, with a normative nature, of the public institution of the *military administration* is stipulated in the "*Decree on the establishment of administrative boards in all the army*"[7], stating that, "*until the publication of the administration and accounting regulations, the military bodies are authorized to carry out the supply through the administration boards*"[8]. At the same time, in act on the formation and organization of the military intendance body, motivating the need to organize their own logistics division of the army, the institution was advocating for the "*need to organize a body of officials responsible with controlling and supervising of all administrative tasks of the army, under the authority and delegation of the deputy Secretary of War, especially wanting to ensure economy in expenditures, proper use of funds and good living of the soldiers*"[9].

Acknowledged as "*greatest importance for the conservation of the defenders of the state*, *and for sparing its income"*[10] as a result of his request from the representative military administration structures, this body has continuously evolved, in relation with the development of the military institution. Afterwards, the new organization of the "Ministry of War", elaborated in 1862, included in its structure a department intended for the "*general administration*", whose purpose lied in providing health services, intendance services, transportation and administration services[11].

In the process of organizational and conceptual crystallization of the military administration, as a public service institution of national defense, the developing of a large number of military rules and regulations, that basically prepared the public awareness of the military administration, was decisive. The most significant of these rules and regulations are:

---

[2] It was promulgated by the High Royal Decree no. 1297, in arch 17th 1937, in the Official Monitor no. 66 from March 20th 1937

[3] The nomination "Carol II" was settled by the Law named "The denomination of the unification Codes of the legislation" decreed under the number 577/1936, published in the Official Monitor, part I, no. 73/27.03.1936

[4] The High Royal Decree no. 471 from March 17th 1936, published in The Official Monitor no. 65 from March 18th 1936.

[5] The Decree-Law no. 2530/1940, published in The Official Monitor no. 194, July 31st 1940

[6] The Military Justice Code "Regele Mihai I", "Universul" newspaper Publishing House, Bucharest, 1941.

[7] "Monitorul Oastei", no. 19, January 28th 1860

[8] *Ibidem*

[9] "Monitorul Oastei", Year II, no. 11, from February 16th 1861, p. 161.

[10] Ibidem, p.168

[11] Maior Ioan Popovici, *Organisarea Armatei Romane*, vol. I, *Schita istorica a organisarei de la 1830-1877*, Partea a II-a, Roman, 1900, p.196

- "*The rules of military commands*", a distinctive chapter of which is attributed to "*general government*"[12], "*Instructions for determining the attributions of the officers of military intendance*"[13], which clearly distinguished between the operative relations amongst the military headquarters and administrative structures, predicting their evolution in the context of the shift from peace to war, in the sense that, if war, "*the commander in chief exercises all the military and administrative authority*"[14];
- "*Instructions on administrative inspection*" [15] , which demanded from "*the control processes of the officer corps, quality, severity and compete honor in the inspections that they effectuate an any company, battalion, regiment or division*";
- "*The rules on militia service*"[16], act organizing and regulating the establishment of boards of administration from the battalion level;
- "*Rules on administration and accounting of the corps*"[17], in which were stipulated "*the tasks of the board members (...), the main duty being to conducting the administration in all its details"*[18]
- There is to mention, the Law for the establishment of the Superior Council of the Ministry of War[19] whose provisions stipulated its existence in the respect that its purpose was "*to help the minister in the administration of the army and in the development and application of military laws and regulations"*[20]

A decisive role in establishing and shaping the military institution, found in the public service of the nation as military administration, had the development, under the auspices od the Constitution of 1866 [21] of the "*Law on the organization of the armed forces*" [22] , conceptually, organizationally and legally enhanced, by legal changes in 1872[23] and 1874[24]. According to this law, which stated unequivocally that "the central body of the organization and administration of the everyday interests if the army is the War Ministry[25], in the active corps of the permanent army it was independently established *the commandment of the administration troops,* which subordinated *the Management Officers Corps, the Field Squadron, the Sanitary Company* and *the Company of administration workers.* But a decisive role in this advocacy has the establishment of the *Central Consultative Committee,* whose duties consist in "*the leadership and management of the army"*[26], and the "*Permanent management committee"*[27], with the role of providing appropriate and operative development of regulations and instructions specific to the structures with management tasks.

In the organizational perspective, but also of the necessity to publically strengthen the military operative structures, the *Law on organizing the commandments of the army*[28] has an important role. Under its auspices "*were established the large units (army corps, division, brigade) as permanent military entities in time of peace, with general staffs, and fixed*

[12] "Monitorul Oastei". An III, no. 37, March 25th 1863.
[13] "Monitorul Oastei", An IV, no. 25/1864.
[14] Ion Dragoman, *The military authority acts*, Lumina Lex Publishing House, Bucharest, 2003, p. 161.
[15] "Monitorul Oastei", an VII, no, 22/1867.
[16] "Monitorul Oastei", an VIII, no. 21/1868.
[17] "Monitorul Oastei", no. 27/1871.
[18] Ion Dragoman, *Op. cit.* p. 163.
[19] "Monitorul Oastei", no. 16/1878.
[20] Ion Dragoman, *Op .cit.* p. 163.
[21] The Monitor. Official Journal of Romania, no. 142, July 13th 1866, pp. 637-658.
[22] "Monitorul Oastei", year XI, no. 21, June 22nd 1868, pp. 257-271.
[23] Ibidem, no. 14, May 26th 1872, pp. 265-275.
[24] Ibidem, no. 14, June 1st 1874, pp. 597-608.
[25] Ibidem, no. 21 June 22nd 1868, p 257.
[26] "Monitorul Oastei", year XIX, no. 21, June 22nd 1868, p. 260.
[27] *Ibidem,* p. 274.
[28] "Monitorul Oastei", year XIII, June 8th/20th 1882, p. 143.

structures, (...) the largest division of the army becoming the army corps"[29]. As consequence of this law, "*the territory was divided in terms of military organization in four major regions, attributed to the new headquarters were the army corps based in Craiova, Bucharest, Galati and Iasi*"[30].

In the functional and conceptual systematic evolution, of the national military administration, the *Law on Military Administration*[31] had a decisive role. This law gives the military issues of the country a systemic character, in agreement with the representative military bodies of the time. In this respect, between the provisions of the law, there are conclusive the matters that axiomatically define the following issues: "*the minister of war is the leader of the army and bears the responsibility of the management of the army*"[32]; "*the administration of the army includes the intendance, the artillery, the engineer troops, the sea troops, sanitary troops, treasury and post services*"[33]; "*the army corps commander has the authority to order according to the laws and ministerial decisions of all the funds and materials allocated to his command, ensuring the exact application of all the laws, regulations and ministerial decisions in all the services*"[34]; "*the divisional commanders have, under the authority of the army corps commander, toward the troops, the establishments and the services in their divisions, the same surveillance duties as the army corps commanders*"[35].

In the same respect, of emphasizing the conceptual and institutional evolution of the military administration, it is enrolled the *Law on organizing the army*[36], from which we withhold that in the chapter about the role of the commandment[37], it was stipulated that the King was the leader of the armed forces[38]; the military administration is lead by the Ministry of War, organized by a special law[39]; and the army corps and division commanders have under their orders all the troops, services and general establishments of the army, as well as all the cities administratively depending on the Ministry of War.[40]

Following the establishment of the National Unitary Romanian State, in the context of Romania's resettlement in the legal and constitutional paradigms of the national unification, the *Law relative to the organization of the army*[41] marks the conceptual condition. From its provisions it is kept in mind: designing a new military organization, according to the new national realities; the establishment of the army general inspectorates through the structural delimitation of the army corps commandments and the division commandments; the strategic division of the territory in seven military regions, corresponding to the seven army corps of the Romanian army; projection of the responsibilities regarding the leadership of the army, the King being the "head of the army, which during war, can delegate the commandment to a general"[42].

---

[29] Maria Georgescu, *History of the General Staff*, 1830-1914, p. 147.
[30] *Ibidem*, p. 179.
[31] "Monitorul Oastei", no. 11/1883, quoted from Ion Dragoman, *Military Authority Acts*, Lumina Lex Publishing House, Bucharest, 2003, p. 156.
[32] *Ibidem*, Art. 1.
[33] *Ibidem*, Art. 2.
[34] *Ibidem*, Art. 7.
[35] *Ibidem*, Art. 9.
[36] "Monitorul Oastei", no. 15/1908, quoted from Ion Dragoman, *Military Authority Acts*, Lumina Lex Publishing House, Bucharest, 2003, p. 171.
[37] *Ibidem*, Cap. X.
[38] *Ibidem*, Art. 35.
[39] *Ibidem* Art. 36.
[40] *Ibidem*, Art. 37.
[41] The Official Monitor no. 134 from June 24th 1924
[42] Costinel Petrache, *The national defense in contemporary Romania. The Political approach*, CTEA Publishing House, Bucharest, 2006, p. 81.

In the pre-World War II terms, it is promulgated the *Decree-Law on organization and functioning of the Ministry of National Defense*[43], which reinforces the conceptual status of the *military administration*, regulating *the general attributions of the Ministry of National Defense*[44], by stipulating responsibilities regarding the leadership, management and the manner to control the land army, and the coordination by the General Staff of the entire system of operations subsumed to the national defense; the *structure, components and the attributions of the senior management, of command and training*[45], mainly of the Deputy Office of the Ministry of National Defense, of the Supreme Council of the Army, of the General Staff, and of the general inspectorates of the army.

In the support of the legal concerns, the issues related to the military administration were in the attention of theorists, in the forefront of the Romanian military thinking. This obvious fact is underlined by a few examples. Thus, in specific military documents, in 1870, the "*Study of the intendance service during campaign*" [46] estimates that "*the military administration, whose goal is the maintenance and conservation of the armies, is one of the important branches of warfare, in the same time being a branch of the public administration*"[47]. The same author, in the "*Short course of military administration"*[48] based on an argument that "*any army aspiring to the honor of being established on solid and durable grounds needs a good administration, different from the commandments ensuring the discipline and training*"[49], affirms: "*Command and administration, here are the ground of the military science, here are the supports on which leaned those armed men whose holy mission is to defend the homeland and homes of their parents, here is at last that secret that makes a lot of individuals move as one, to work and tremble under the impulses of a single head*"[50]. Very interesting, in terms of their conceptual vision, are the assessments of Mr. Sergie Voinescu[51] according to which "*the commandment is a head with more arms: the head is the general, and the arms are the general staff*"[52], noting that "*too many in peacetime, officers are insufficient in wartime*"[53]. We find both interesting and useful the establishment of the concept that states: "*one branch of the public administration is the military administration, which covers the maintenance and the preservation of armies, being one of the major branches of the art of war, led by a officer corps, called military intendance*"[54].

A very special contribution on the theoretical front of the conceptual development and thus, applied to military administration, with determinations in doctrinal development of military administrative law, had Colonel, Vasile D. Chiru.

Prodigious theorist, in law and military justice, Vasile D. Chiru, leaned over the condition, significance and importance of the military administration, as an extensive area of the organization, support and military action. From his referential studies[55], the most important are thesis like: the applied need of separation and specialization of the executive bodies, "the

---

[43] Cioflina Dumitru, Osca Alexandru, *History of the Romanian General Staff. Documents*, 1859, 1947, Military Publishing House, Bucharest, 1994, p. 280.
[44] *Ibidem*, Title I, p. 281.
[45] Ibidem, Title II, p. 287.
[46] Adj.Cls.I Constantin Movila, *Study on the intendance service during campaign*, Monitorul Oastei, no. 27/1870
[47] *Ibidem*, p. 211.
[48] "Monitorul Oastei", no. 28/1872, pp. 83-197.
[49] "Monitorul Oastei", no. 28/1972, paraphrased by Ion Dragoman, *Military Authority Acts*, Lumina Lex Publishing House, Bucharest, 2003, p. 181.
[50] "Monitorul Oastei", no. 28/1872, p. 84.
[51] Mr. Sergie Voinescu, *Study of the general staff in battle,* Monitorul Oastei, no. 10/1883, pp. 42-65.
[52] *Ibidem*, p. 45.
[53] *Ibidem*, p. 57.
[54] Dimitrie Mihailescu, *Course od legislation and administration*, Goldsleger Printing House, Botosani, 1889, quoted by Ion Dragoman, *The Military Authority Acts*, Lumina Lex Publishing House, Bucharest, 2003, p. 183.
[55] Chiru, V., *Commandment and administration*, Curierul Justitiei Militare Publishing House, Sibiu, 1934.

problem of administrative separation being required nor only for the fighting army, where the fates of the administration merge with the commandment, but also for the other units and departments of the army, for which the administrative separation is an absolute requirement of the times" [56]; the creation of an administrative body, thoroughly specialized in total committing to administrative facts and deeds, so that the combatant military component, designated for preparing for battle and combat to be relieved of any further responsibility, other than those resulting from the nature of their combat mission. In another paper[57], advocating for a clear delineation between commandment and administrative deeds, he sanctioned "*the error in conception of the combat officers (...) perpetuated to this day*"[58], that " *military administration issues were considered minor matter, addressed by the assimilated, managers and intendants, this being their duty, and for the administrative duties regarding the subunits, the skills of the sergeant were more than enough*"[59].

3. The decisional support of the military administration

The central bodies of the military administration, and the deconcentrated bodies of the military administration represent the decisional support of the military administration institutionally, structurally and technically. We will refer to these institutions in the following chapter, describing their main duties and responsibilities.

The question that arises targets not only the anatomy of the decisional act, in this case the institutional support, but also its physiology, in where we find the administrative and commandment deeds of the military administration, according to the levels of functioning, implicitly the acts of military and politico-military responsibility, actions possible to be undertaken as a result of the decision making process. From this perspective, in an extended comprehension, I appreciate that from a conceptual point of view, *the decisional support of the military administration* is configured super-structurally, by all the ideas, theories, concepts, and doctrines specific to the nature of the military administration and to the relations determined by it, which by institutional consecration, make possible the projection and accomplishment of the acts and deeds of military administration. In the development process of the decisional support of the military administration, of the decision itself, a very important role has the decisional support, expressed by the totality of administrative and commandment actions, which come in the support of making a decision, as a result of considering a problem, incurred by a practical situation.

The central bodies of the military administration

Strictly in terms of conceptual, organizational and systemic relation with the central administration, the *central bodies of the central bodies of the military administration* are: The General Staff, the departments and the central directorates of the Ministry of National Defense and the Staffs of Services. The acts and deeds of command, but also of administration of the *central bodies of the military administration* have a strategic character and are purely military. According to the law[60], in the category of the central bodies of the Ministry of National Defense there are admitted: the Department for Defense Policy and Planning, the Department for Parliament Liaison and Public Relations, the Armament Department, the General Staff, the General Secretariat, the Defense Intelligence General

[56] *Ibidem*, p. 5.
[57] Chiru, V., *Military Administrative Law*, Curierul Justitiei Militare Publishing House, Sibiu, 1936.
[58] *Ibidem*, p. 4.
[59] *Ibidem*, P. 5.
[60] Law no. 346, from July 21st 2006, regarding the organization and functioning of the Ministry of Defense, published in the Official Monitor no. 654 from July 28th 2006, with the subsequent modifications, Art. 6, alin. (1).

Directorate, Human Resources Management Directorate, Financial – Accounting Directorate, the Control and Inspection Corps, Internal Audit Directorate and the Medical Assistance Directorate.

Next, the main commandment acts and deeds of the General Staff, and the administrative acts and deeds of the central departments of the military administration will be outlined.

- *The General Staff* – Is the central administration body, with the most important attributions, purely military, in the field of national defense, basically by the command acts and deeds that were intended, managing the entire procedural armed defense of the country. From the perspective of legal[61] provisions that shape the public role of the General Staff in the national military administration, the only one with a well shaped role of central administrative body, the attributions are generated by the responsibility invested to ensure:
    - The leadership, organization, planning and operationalization of the forces;
    - Gradually raising of the combat capacity and mobilization of the army;
    - Conducting joint operations and management of operational logistics support;
    - Training the commandments and troops and basic and special training of the active and reserve military personnel;
    - Individual career management of military personnel;
    - Planning the equipment of the force structure;
    - Defining the necessary military equipment under measures and operational requirements and standardization in the military system;
    - Implementation of the command, control, communications, computers, information, computer, surveillance and reconnaissance;
    - Cooperation with foreign armed forces and the deployment of international military relations;
    - Technical agreements with the armies of other states and international organizations to which Romania is member;
    - Religious assistance in Ministry of National Defense and promoting the values of specific military traditions, military culture, civic education and military ceremonies.

Simultaneously, in terms of its mission a central body of military administration, the General Staff has responsibilities on:

- Organizing the training of ministers, secretaries, and deputy secretaries of the Ministry, as well as the officials with their corresponding rank, prefects, deputy prefects, and officials with executive responsibilities in the central or local administration, in order to fulfill their duties in the line of national defense;
- Approval of the documentation of the ministries, public authorities and economic institutions regarding the development of new projects and the development of the existing infrastructure in order to comply with the national defense system;
- Quantification, and maximize operational management of the lines of action in defense, namely: the fight against terrorism; combating the proliferation of weapons of mass destruction; military transformation; crisis management; information for defense; economy and defense industry; enhancing and developing the potential of cultural, scientific and human resources of Romania; permanent employment of concern for environmental protection and ecological security; efficient management of resources for defense;

[61] *Ibidem*, Art. 12, alin (1)

- Operational management of special operations forces, and in case of participation in military operations outside the national state, according to technical agreements concluded with foreign partners;
- Approving the annual objectives and territorial defense preparation program
- Periodically check the status of preparation of the population, economy and territory for defense, through mobilization exercises and training;
- Development the legal framework, the leadership, guidance and control of the activities of military records of citizens and military reservists, throughout the national territory.

- *The Department for Defense Policy and Planning* – The fundamental institutional mission of the Department lies in coordinating the assumed international obligations, defense policy and integrate defense planning enforcement and coordinating the political-military international cooperation.[62]
- *The Department for Parliament Liaison and Public Affairs* - Department of Parliament Liaison and Public Information - Essential coordinates relationship with Parliament and legislative work, providing legal assistance and represents the interests of the Ministry of Defense before the courts and other organs of judicial activity, ensure relations with other public authorities and NGOs, guide the harmonization of the laws and provide legal assistance for technical agreements for cooperation with foreign armed forces, leads activities concerning public information and military media, deals with issues regarding the legal regime of the property of the Ministry of National Defense and coordinates the activity of solving social problems of staff[63].
- *The Armaments Department* – Develops and coordinates the procurement policies of the Ministry, as the regulatory authority in the field, manages relations with national defense industry, provides program management for procurement of major weapon systems and equipment and related contracts and of research and development, plans and operates international armaments cooperation, performs quality monitoring at the military equipment suppliers, coordinate the training and retraining of officers specialized in technical engineering logistics and other specialists needed in the military organization, preforms the metrology and technical standardization works and effectuates the specific control for the import and export of special products[64].

The deconcentrated bodies of the military administration

Deconcentrated bodies of the military administrations are assimilated to the military structures that perform command acts and deeds, of operational or tactical nature. Basically, in terms of organization, responsibility and specific mode of action, in general, the deconcentrated bodies of the military administration comprise the territorial commandments, division commandments, brigades, battalions and various configurations with auxiliary role in the preparation for battle.

Without underestimating the importance of all the deconcentrated bodies of the military administration, for the conceptual clarifying, only those belonging to the category of Army forces will be mentioned.

- *The Staff of the Army*[65]
  - 3 Infantry Divisions, each comprising combat brigades, support regiments, a logistics base, combat support battalions, and a logistic support battalion;

[62] *Ibidem*, Art. 8.
[63] *Ibidem*, Art 9.
[64] *Ibidem*, Art 19.
[65] https://www.forter.ro/content/structura

- Combat support brigades; combat support and logistical support centers; a training center for combat ground forces; combat support and logistical support battalions; training and shooting ranges; educational structures (Army Academy, Military School, Non-Commissioned Officers School, weapons application schools, Military Colleges)

- *The Staff of the Air Force*[66]
  - Air Bases 71, 86 and 95, Base 90 Transport, 1st Brigade-air missiles, 91 Base Logistics, Regiment 70 Aviation Engineering, Center 85 Aero Communications and Informatics, Air Operations Center, Launch Site "Capu Midia", education structures and units (Air Force Academy, Air Force Non-Commissioned Officers School, schools of applications)
- *The Staff of the Navy*[67]
  - The fleet, composed of: Frigate Flotilla, Naval Missile Battalion 150, Division 50 Corvettes, 146 Division Mining-Demining Ships, Battalion 110 Communications and Information, River Service, 67 Carrying Artillery Ships Battalion, Division 88 River Gunboats.
  - Naval Logistics Base: Divisional special ships, Naval Technical Maintenance Center 338; Sections 335, 329, 330 and 325 Logistics, located in Constanta, Braila, Constanta and Tulcea.
  - Education and culture institutions: Naval Academy, Military Marine Training School, Application School, and Navy Museum.
  - Specialized structures: Diving Center, Radio-Observation and Radio-electric Center "Callatis", Computer Center, Training, simulation and evaluation Center, Marine Hydrographic Department, Marine Naval Medical Center, Marine infantry Battalion 307, Navy Support Battalion.

To these we add the *military territorial bodies* that comprise regional military commands, county, municipal and sector military centers[68].

As role and attribution, generally, the deconcentrated military administration bodies: transmit or, as applicable, perform orders and provisions from the upper echelons; organize, lead and conduct outreach and tactical applications, command training regime; participates and manages the training of local public administration officials through regular attendance at meetings; organizes and carries out activities to promote the profession and military career, and in certain cases, established by the superior bodies, perform recruitment activities; perform specific activities of military and reserve personnel training; performs specialized activities of military training for the staff; systematically verifies the compliance of their obligations by the entrepreneurs in order to implement the tasks form the mobilization documents.

4. Public administration and authorities. Operational interdependencies

In the conceptual support of the theoretical ideas engaged, this paper will briefly treat, aspects, which fulfill by being complementary the comprehensive understanding of the decisional support of the military administration. A first aspect is represented by the correlation between the public and central administration in peace, crisis, and war time, as well as between the public administration and the military administration. From the constitutional point of view, the definitions of these notions are clear, in this respect they target:

[66] https://www.afahc.ro
[67] http://www.navy.ro/
[68] National Defense Law, Art. 10

- *public authorities* [69] which include the Parliament, the Presidency and the Government;
- *central public special administration* [70] whose structure [71] includes the ministries organized exclusively subordinated to the Government, as well as other special bodies organized either subordinated to the Government or the ministries, or autonomous administrative authorities;
- *local public administration* [72] organized by administrative-territorial principles, exercised by communal councils, city councils, municipal councils (Bucharest council), county councils, all being deliberative authorities, and the mayors as executive authorities.

The distinctive relation between the central public administration and the local public administration, whose general leadership is exercised by the Government[73], is highlighted by a number of criteria expressed by: material and territorial competence of the public administration bodies and the nature of the communitarian interest they represent; the difference in scale between the two scales of the public administration, the central administration exercising its competences over all the national territory, the local public administration exercising its competences and attributions in the administrative units in which they were democratically invested by the communities.

Absolutely natural, between the military administration and the public administration, vital vectors of the social system, there are established essential and necessary, interdependent relationships with finality in maximizing each other's institutional role. The complexity and the functional nature of social relations between the military administration and the public administration are distinguished by thoroughness of the related legislation and the content of some provisions of the constitutional act. However, the nature and, in particular, the extent of these relationships is evident by the institutional engagement, in the military administration spectrum, depending on the specific conditions under which this can occur, respectively at peace, in crisis, or in the event of war, after the state of siege. This administrative-institutional engagement requires a thoroughly planned coordination of the national defense, goal assumed by organic law [74]. From a constitutional perspective of military administration, defense planning is "an essential component and attribute of the defense policy" and "is a complex of activities and measures aimed at promoting national interests and objectives defining Romania's national security defense"[75]. The defense planning, responsibility of the military administration, "is based on political decisions of the President, Parliament and Government of Romania and the measures and actions taken by other institutions, which, according to law, have responsibilities in the field of defense"[76], "the National Defense Strategy of Romania being the basic document which entitles the defense planning at national level"[77].

The national dimension of the responsibilities arising from the complexity of the defense planning, attributes assigned to the military administration, requires in fact the existence of the *National Command Authority*[78]. Non-formal institution, which by the total

[69] The Romanian Constitution, Title III, published in the Official Monitor no.767, 31st October 2003
[70] *Ibidem*, Chapter V, Section 1
[71] *Ibidem*, Art 116
[72] *Ibidem*, Section 2
[73] *Ibidem*, Cap III, Art 102
[74] Law no. 473, 4th of Nov 2004, regarding defense planning, The Official Monitor no. 1052, 12th of November 2004
[75] *Ibidem*, Art.1
[76] *Ibidem*, Art.3
[77] *Ibidem*, Art.4
[78] Badalan, E., *The military administration, Course Notes*, Terrestrial Forces Academy Publishing House, Sibiu, 2004, p. 54.

amount of direct responsibilities in defense, can be linked, forcing somewhat the concept, with a military para-administration, is composed of the Parliament, the Presidency, the Government and the Supreme Council of National Defense.

The expositive highlighting of the nodal components of the National Commend Authority, constitutionally having the quality of *public authorities* or *special central public administration authorities*, in the context of legal determinations ne defense planning, questions the necessity of the interdependent relationship between the *public administration* and the *military administration*, helping to structure on one side the operational objectives of the military administration and the preparation of their materialization, and on the other side the definition of specific opportunities to execute them.

This interdependence necessarily and functionally imposes issues referring to:

- Materializing the possibility of using the elements of the communication system in cases of force majeure, well defined by operational procedures of the military administration;
- Designing specific doctrines for each of the Army forces, as well as joint doctrines, regulations and standards specific to the defense operations, in line with the diversified potential managed by the public administration;
- The maximum efficiency use of the economic environment, resorting to outsourcing of activities;
- Coordination and control of the entire defense efforts, continuous and uniform;
- Relieving the headquarters of large military units through operational outsourcing of services and taking them over by local or central bodies of public administration, which is possible by employing modular logistic forces;
- Continuous improvement of collaboration activities on concrete objectives of common responsibilities regarding the national defense, between the military administration structures and the public administration structures;
- The systematic optimization of communication at all levels of institutional and organizational defining, between the operative structures of the military administration and the public administration;
- The most efficient use of the financial, material and other nature resources, by applying centralized procurement procedures;
- Standardizing the procedures relating to actions carried out jointly by the public administration and the military administration, especially those that involve the actual enforcing of national legislation in the military field, specifically through dispositive and provider actions;
- Establishing and clearly defining the responsibilities and activities that can be transferred to the jurisdiction of central or local government bodies in order to maximize response time in special situations, but also the efficient use of the resource at any time.

All this truly inter-relational system, striking out civil-military relations, on the quality of which decisively depends the response of the state at any of the situations arising from possible external threats to peace in situations of crisis and war, or from the declaration of the state of siege.

Without excessively detailing the raised issues, it can be appreciated that the nature of the civil-military relations, in the context of the state of siege, are highlighted by the very definition of the *state of siege* which "*represents all the exceptional measures of political, military, economic, social and other nature, applicable in the entire territory of the country or just in some administrative-territorial units, established for the country's defense capacity adjustment to serious danger, current or imminent, threatening sovereignty, independence,*

unity or territorial integrity of the state"[79], situation in which "*exceptional measures can be enforced, applicable in the entire territory of the country or just in some administrative-territorial units*"[80].

Conclusions

Since its establishment on modern grounds, the Romanian military body corresponded to the operational requirements of the condition of the military administration, exercising both command attributions but also specific administrative acts, in the most institutional meaning. Moreover, even if just minimal examples were used in advocating this subject, we consider that during the period that defined the evolution of the Romanian state since its establishment in 1859, until the moment Romania entered the totalitarian social evolution paradigm, a true legal doctrine relative to the military administration was crystalized.

The General Staff is the main and most important institution of the military administration, the only one whose acts and deeds have purely military strategic character.

The central military administration bodies not only adopt not only major decisions proper to the military institution, but also administrative and command acts and deeds for setting in place of defense political-military strategies.

It is confirmed that the decisional institutional support of the military administration consists of all the military structures that are part of the central and deconcentrated bodies of the military administration.

The relations between central and local public administration bodies, one hand, and central and central and decentralized military administration bodies on the other hand, are significantly determined by the operational quality of institutional relations but also by the social civil-military relations.

BIBLIOGRAPHY:

1. Bădălan, E., The military administration, Course Notes, Terrestrial Forces Academy Publishing House, Sibiu, 2004
2. Chiru, V., *Commandment and administration*, Curierul Justitiei Militare Publishing House, Sibiu, 1934
3. Chiru, V., *Military Administrative Law*, Curierul Justitiei Militare Publishing House, Sibiu, 1936
4. Cioflina, D., Osca, A., History of the Romanian General Staff. Documents, 1859, 1947, Military Publishing House, Bucharest, 1994
5. Dragoman, I., *The military authority acts*, Lumina Lex Publishing House, Bucharest, 2003
6. Georgescu, M., *History of the General Staff*, 1830-1914
7. Mihailescu, D., *Course od legislation and administration*, Goldsleger Printing House, Botosani, 1889, quoted by Ion Dragoman, *The Military Authority Acts*, Lumina Lex Publishing House, Bucharest, 2003
8. Movila, C., Study on the intendance service during campaign, Monitorul Oastei, no. 27/1870

[79] Law 453, regarding the state of siege and the emergency state regime, The Official Monitor no.1052, 12th November 2004, Art. 2.
[80] *Ibidem.*

9. Petrache, C., *The national defense in contemporary Romania. The Political approach*, CTEA Publishing House, Bucharest, 2006
10. Popovici, I., Organisarea Armatei Romane, vol. I, Schita istorica a organisarei de la 1830-1877, Partea a II-a, Roman, 1900
11. The Military Justice Code "Regele Mihai I", "Universul" newspaper Publishing House, Bucharest, 1941
12. Voinescu, S. *Study of the general staff in battle,*Monitorul Oastei, no. 10/1883

Legislation
1. "Monitorul Oastei" form 1860, 1861, 1863, 1864, 1866, 1867, 1868, 1871, 1873, 1882, 1908, 1924
2. The Official Monitor from 1924, 1936, 1937, 1940
3. Law no. 346, from July 21st 2006, regarding the organization and functioning of the Ministry of Defense, published in the Official Monitor no. 654 from July 28th 2006, with the subsequent modifications
4. Law 453, regarding the state of siege and the emergency state regime, The Official Monitor no.1052, 12th November 2004
5. Law no. 473, 4th of Nov 2004, regarding defense planning, The Official Monitor no. 1052, 12th of November 2004
6. , Romania's national Defense Law no. 45 from July 1st 1994, the Official Monitor no. 172, July 7th 1994
7. The Romanian Constitution, Title III, published in the Official Monitor no.767, 31st October 2003

Web Resources
1. https://www.forter.ro/content/structura, acessed between March 20 and March 30 2015
2. https://www.afahc.ro acessed between March 20 and March 30 2015
3. http://www.navy.ro/ acessed between March 20 and March 30 2015

COUNTER-HYBRID WARFARE. DEVELOPMENTS AND WAYS OF COUNTERACTING HYBRID THREATS / WAR

Marian RĂDULESCU
Lieutenant colonel, Superior instructor, NCO "BASARAB I"Academy, Pitesti, Romania,
e-mail: mradulescu1969@yahoo.com

***Abstract**: The international security environment underwent major changes, generating strategies of adaptation, state capacities, including military, transforming organizations involved in regional and global security, to counter new risks and threats.*

New, asymmetric threats, exceed the conventional war, being of a military level (guerrilla, civil war, terrorism, insurgency) and also non-military (organized crime, murders, political, economic, psychological, media, information assaults, cyber, climatic, geophysical war, ethnic separatism etc.).

A distinct challenge for NATO and its partners consists of hybrid threats that combine innovatively the effects of conventional means with the irregular, asymmetric ones, the threats source being largely non-state actors, with the support of partner countries, from behind.

Hybrid Warfare Counter issue requires a comprehensive, consistent and coherent approach in all elements of state, regional and international power to discourage this type of threat, identify and facilitate pro-active response measured at strategic, operational and tactical level.

***Keywords:** hybrid, asymmetric, unconventional threats, NATO, operational planning, special operations.*

Introduction

The international security environment coagulates new elements of risk and threat: demographic change, energy crisis, climate change, economic crisis, the spatial dimension of the war, increasing the importance of non-military aspects, accessibility to information, leading military technology migration by illegitimate powers, separatism ethnic and religious.

Avoiding confrontation classical to decrease conventional military superiority of modern armed, non-state actors, organizations and even countries successfully uses complex methods of warfare, which circumvent or defy the laws of armed conflict, combining forces, lethal and non-lethal means, conventional fighting tactics with the unconventional, including terrorist attacks, assassinations, information operations and cyber attacks, designs battle space in the media, in large disinformation and propaganda, trying to legitimize their actions and weaken the enemy power.

Easy access to high-tech military equipment, terrorist organizations with advanced weapons systems, normally associated, conventional armies, propensity to operate in urban, densely populated areas tend to combine in a synergistic technologies, military action political, media, and to influence public opinion outlines future conflicts.

The "unrestricted warfare" practiced by terrorist organizations, state and non-state actors is complemented by exploiting the presence of civilians in the conflict zone by deliberate action to increase the number of victims of collateral, in violation of the principles of LOAC (Law of Armed Conflict). This was followed by altering the information channels, falsifying reality, military operations, otherwise legitimate, the opposing party, as being disproportioned, in order to influence and achieve strategic advantage.

These actors substantially alter the operational framework of the war, for which groups of regular forces must adapt technologies, organizational structure, strategies, tactics and procedures for action.

1. Doctrinal ideas on hybrid war

Analyzing recent conflicts, academics, planners and military commanders have anticipated environment confrontation trends, threats and thus trying to define the types of current and future wars. There were such concepts Unconventional warfare, irregular warfare, and, more recently, hybrid warfare. If the first military specialists' opinions are convergent concepts, generating effective response strategies, hybrid warfare knows different interpretations and shades.

1.1 Conceptual

The concept of hybrid threat is operational art's evolution, bringing considerable potential doctrinal and organizational revolution in military affairs. This term arose after the conflict in Lebanon (2006) between Israel and Hezbollah, from the necessity of increasing the description of non-linear threats of state and non-state actors.

Seen as a sophisticated amalgam of ways, means, techniques and unrestricted methods, whereby state and non-state actors innovatively combines and simultaneously regular and irregular capabilities to create strategic effects, proliferation threats hybride led to much debate. The debate on hybrid threats is supported by the lack of a universally accepted definition.

In 1996 historian Thomas Huber advanced the term "war compound" to describe the mixture of regular and irregular forces fighting for a common goal.

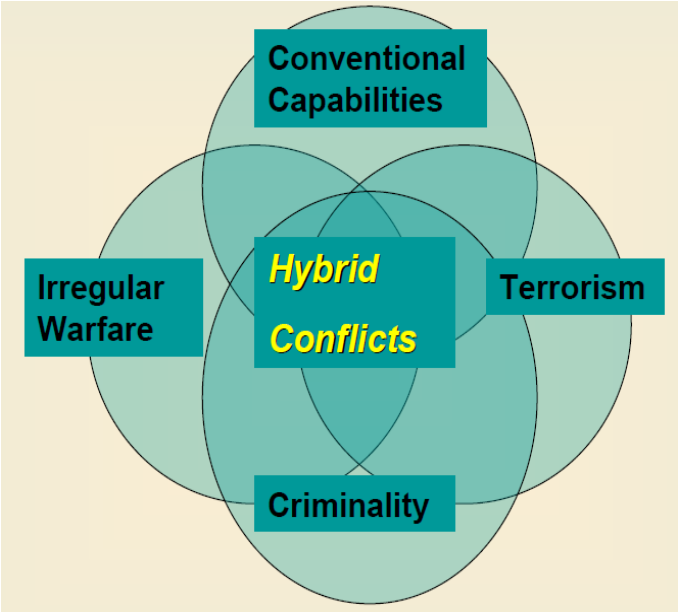


Figure no. 1. Future conflicts according to Hoffman[1]

A key role in defining and developing the concept was played by Frank G. Hoffman. In the article Future Warfare: The Rise of Hybrid Wars (2005), the author shows that although conventional war will not disappear, armed forces maintaining capabilities to waging a major operation, it is necessary to enact detailed response in case of new threats, hybrid. He considers that various forms of war can be used simultaneously. Non-state actors mostly used forms of irregular warfare, but will support participation in a conventional conflict, if it serves their purposes.

In the paper Conflict in the 21st Century: The Rise of Hybrid Wars, published two years later, Frank Hoffman examines Hezbollah against Israel Defense Forces actions (IDF) in the 2006 campaign, showing the growing ability of Hezbollah to successfully use

[1] Available at http://indianstrategicknowledgeonline.com/web/DIRIWCSCBriefv3.pdf, accessed at 01.04.2015

capabilities, tactics and diffuse methods in densely populated areas, which combine in a complex characteristics of conventional and unconventional operations. According to the author, in a hybrid war, opposing parties aim to achieve victory through the merge of irregular tactics and the most lethal means at hand, in order to attack the opponent and fulfill their political objectives"[2].

In 2009, in the article "Hybrid vs. compound war", Frank Hoffman discusses the concept of compound warfare launched by Thomas Huber, saying that it assumes the existence of two distinct forces (regular and irregular) working in different parts of the battle, but not to be combined in battle. Irregular forces are used in this situation for wear and actions to support a strategy of exhaustion, paving the way for successful conventional forces. On the other hand, hybrid threats appear to have a greater degree of coordination and operational and tactical combination, with virtually a single force under a single command, acting concentrated by means of conventional and unconventional for a strategic objective.

Dr. Russell Glenn, a renowned military analyst, expands the debate of war compound and hybrid threats. He interprets the war compound as a combined synergistic and strategic level, but not of the the complexity and simultaneity performed at the operational and tactical level, the combined forces of the whole range of methods and modes of action in the battlespace.

Russell Glenn hybrid type defines threat as coming from a "simultaneous actions opponent who adopts political, military, economic, and social information and methods of conventional warfare, irregular, terrorist and criminal acts"[3], which can be a combination of state and non-state actors. In a broader sense, the threat is seen as a hybrid type any natural or manmade incident, including terrorism, resulting in a large number of casualties, extensive damage or disruption severely affecting the population, infrastructure, environment, economy, morale national or functioning state institutions.

In 1999, Qiao Liang and Wang Xiangsui Unrestricted Warfare paper presents innovative alternatives to traditional military employment, using a variety of means without restrictions. They argue that the new approach allows finding alternative ways to cope with the rising costs of conventional warfare. They advocate for forming a composite force, combining military and non-military methods, including the legal and economic belonging to place an opponent at a disadvantage in direct military confrontation.

David Kilcullen in his book "Out of the Mountains: The Coming Age of the Urban Guerrilla" offers a revolutionary perspective on hybrid war, highlighting four megatrends on the evolution of human society: changing population structure, urbanization, increasing the role of coastal, connectivity.

Kilcullen argues that future conflicts may occur in coastal cities, suburban localities, suggesting that cities rather than countries, are critical units of analysis for future conflicts (fair observation, since 2050 about 75% of world population will be urbanized). The degradation of environmental conditions, competition for resources and space, lack of minimal living, difficulties in ensuring an acceptable level of education and health, proliferation of criminal networks could turn large parts of urban highly-densed areas into "territories of anyone". When addressing the issue of urban conflicts, flexibility is required, as only a military solution is unspecified. Involving local people in areas such as urban planning, systems engineering, conflict resolution and mediation is more about issues related to sustainable development policies.

---

[2] HOFFMAN, Frank, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies, 2007, p. 29.

[3] RUSSELL, Glenn, *Evolution and Conflict: Summary of the 2008 Israel Defense Forces*, available at https://www.doria.fi/bitstream/handle/10024/92639/Y2622_HuovinenKPO_YEK56.pdf, accessed at 01.04.2015

According to NATO, "hybrid threats are posed by opponents, the ability to use both conventional and unconventional means of an adaptive manner to achieve its objectives".[4]

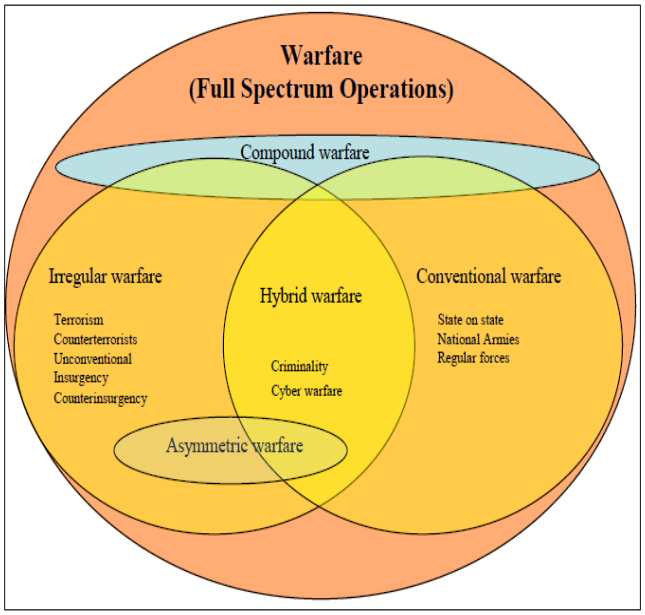


Figure nr. 2. Full spectrum operations [5]

The issue of hybrid war came to the attention of the US Department of Defense officials, who correctly defined the characteristics and peculiarities of this type of conflict. According to Air Force officials, hybrid warfare is more powerful and complex than irregular warfare because the tempo increased complexity and variety of events, characterized by easy access to communications and resources of the opponents. Officials Special Operations Command, Navy and Marine Corps believes that hybrid warfare includes conventional and unconventional forms of warfare, combat the threat potential is covered in terms of doctrine of full spectrum operations.

Given the views expressed above, we consider that hybrid warfare is that form of war based on a flexible strategy that combines innovative conventional, irregular, terrorist and criminal capabilities, integrating simultaneously military, paramilitary and civil[6] forces of some state or non-state actors, exploiting vulnerabilities opposing party, to achieve strategic effects.

1.2 The need to adopt a Counter-Hybrid Warfare doctrine

Margaret S. Bond, in Hybrid War: A New Paradigm for Stability Operations in Failing States[7] describes hybrid war from a broad strategic perspective, through the ungoverned spaces. This paper proposes the need to adopt a new strategic concept for the operation of US forces in non-permissive environments in failed states, where the government has no effective control over its territory and does not provide national security or basic public services for citizens and non-controlling armed forces.

Future war will be, according to the author, a hybrid war, which involves the design of all elements of national power along a continuum of simultaneous activities, from humanitarian missions, military action, stability operations, security and reconstruction. It includes a wide range of conventional forces, military intelligence capabilities, unconventional weapons, support units, combat equipment available for rapid deployment if regular or irregular items adverse forces, terrorist organizations or other state actors or non-state above a certain threshold of hostility and constitute a direct threat.

---

[4] IMSM-0292-2010, *Hybrid threats description and context*, 2010, available at http://cco.dodlive.mil/files/2014/02/Prism_111-124_Aaronson-Diessen.pdf, accessed at 01.04.2015

[5] HUOVINEN, Petri, *Hybrid warfare – Just a Twist of Compound Warfare?*, available at https://www.doria.fi/bitstream/handle/10024/74215/E4081_HuovinenKPO_EUK63.pdf, accessed at 01.04.2015

[6] Some criminal activities can be included as part of the own hybrid war as destabilizing government, or supporting insurgent forces by providing resources (derived from the proceeds of smuggling, drug trafficking, illicit trade, transfers of ammunition or advanced weapons, exploitation urban criminal networks)

[7] BOND, Margaret, *Hybrid war: a new paradigm for stability operations in failing states*, available at http://www.dtic.mil/dtic/tr/fulltext/u2/a468398.pdf, accessed at 25.03.2015

The Future Character of Conflict Paper document (FCOC) [8] developed by the British Ministry of Defense shall forward the idea that the hybrid nature of their future conflicts will increase significantly. The paper explains that hybrid threats can not be opposed to counterinsurgency and stability operations. The main idea is that a hybrid threat aims to exploit opponent weaknesses, combining conventional methods, irregular and asymmetric threats at the same time and space, including economic, financial, legal and diplomatic.

Hybrid Warfare Counter C-HW Counter-Terrorism differs from (CT) or Counter Insurgency (COIN). CT operations tend to be carried out in the short term and the results are visible immediately. C-HW, by contrast, is a proactive doctrine, involving direct and indirect operations holding of a long time, like the attrition war.

COIN operations have a significant kinetic load, contain a substantial physical footprint, aiming to defeat insurgent formations, while the C-HW operations combine direct and indirect methods, military and otherwise, made by (sub) different units as nature, value, organization, in order to prohibit the possibility of the enemy to exploit its own vulnerabilities, to concentrate its capabilities to achieve synergistic effects, public support in the conflict and the necessary conditions for achieving strategic success.

The war in Gaza (2014) has proved insufficient Counter-Terrorism concepts such as Counter-Insurcency, or effects-based operations (EBO) in a hybrid war, being necessary to develop a distinct doctrine that addresses this type of conflict.

Extending the conflict in Afghanistan and Iraq revealed a systemic failure on counterinsurgency operations, by developing appropriate remedy, in 2006, of a new counterinsurgency manual FM 3-2 and by training forces in planning and executing this type of operation. Regarding new threats, United States Army Special Operations Command designed in September 2014 *Counter Unconventional Warfare - White Paper*, that could be pivotal in adopting a C-HW doctrine. It is important not to put equal sign between C and C-HW-UW, UW since C does not address all threats and not all threats are unconventional.

2. Directions and ways to counter the hybrid threats

Shaped by the actions of Iran in the Middle East and the Chinese by the concept of unrestricted warfare, hybrid war is now the "solution" adopted by the separatist insurgents in Ukraine. This type of war, characterized by integrating traditional and unconventional actions completed by the conflict extension to the economic, civil, diplomatic, cultural, media and informational fields, to which may be added destruction of critical crime or attacks with weapons of mass destruction requires vigorous action, preventive, convergent, based on a specific doctrine that addresses the full range of threats, which includes political-military strategic direction of action. This will allow preventive measures and coherent response, undertaken by the entire society and implemented by institutions with security.

2.1 Comprehensive approach to all elements of power

Countering hybrid threats therefore requires a comprehensive approach to all elements of power. Cooperation between institutions, government agencies and non-governmental organizations, regional and global security, military, intelligence agencies is vital to adopt active measures to prevent and respond threats: military actions, political and diplomatic measures, economic sanctions, support from the partner nations and organizations, strategic information to expose the threat.

[8] ***, Ministry of Defence UK, *Future Character of Conflict Paper (FCOC),* disponibil la adresa https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/33685/FCOCReadactedFinalWeb.pdf, accesat la 23.03.2015

A national capacity C-HW is a long-term option and depends on the willingness of leaders to engage elements of national power in prolonged operations, conducted in sensitive environments, including hiring armed forces in military actions of wear.

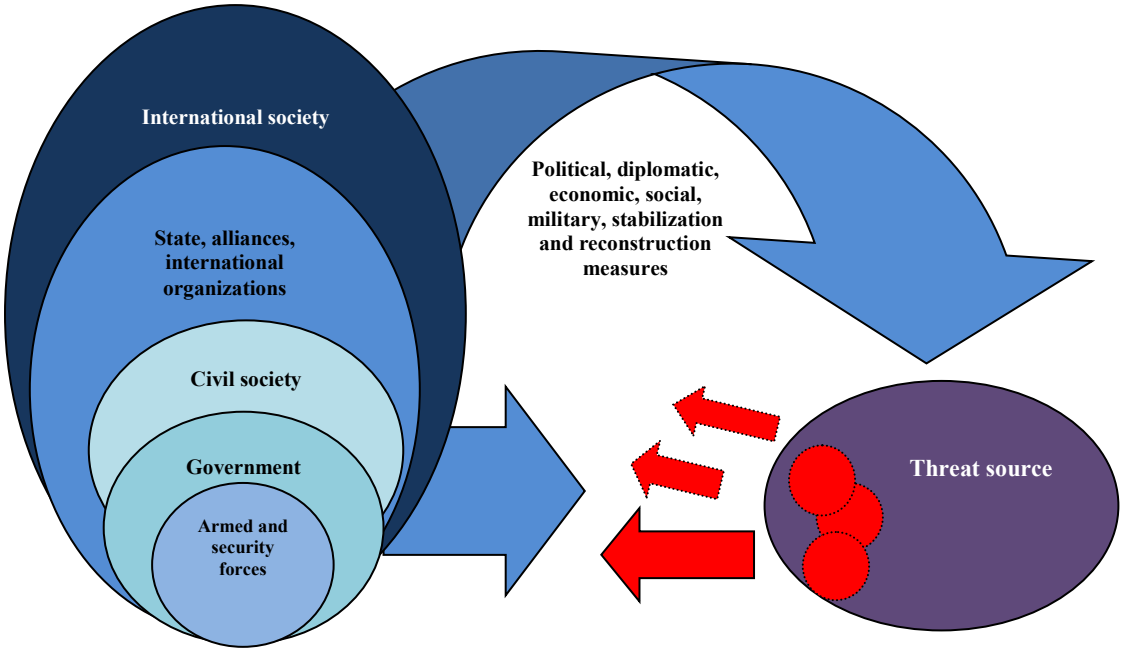


Figure no. 3. Comprehensive approach to hybrid threat

Nations must be able to adapt their national strategies, mechanisms for cooperation, and the concepts of struggle and force structures, adaptive and efficient to combine all civilian and military capabilities to reduce all risks and threats that bring major disruptions and that lead to conflicts, which can be, in most cases, hybrid type.

At a strategic level, coordination and synchronization of efforts to achieve the general objectives could be insured by a mixed group of interagency coordination, personnel of the armed forces and representatives of other ministries, institutions and agencies. At the tactical level, interagency coordination could be provided by linking officers (LNOs).

Based on the description of the threat, a doctrine of Counter-Hybrid Threats / Warfare must be developed, which can be implemented based on concepts, procedures, planning documents and important changes in force structure.

2.2 A new approach to planning military operations

After the Cold War, the military community has tried to define the types of threat, many ideas describing the complexity and the tendency of changing the operational environment, as old doctrine became obsolete. The concepts developed in recent decades have defined the planning of military operations in accordance with the operating environment changes. Among these, there are Fourth Generation Warfare, Network-Centric Warfare, Counter-Terrorism and Counter-Insurgency (COIN).

Conflicts in the future will be characterized not only by conventional or irregular actions. Opponents will use ingeniously combination of traditional, irregular and disruptive to achieve operational and strategic advantage. Therefore, the hybrid threat provides a framework to describe the evolving nature of threats, challenges conventional methodologies for assessing threats and highlights the dynamics of contemporary operational environment.

Hybrid threats provides challenges for operational and strategic military planning. Chaotic and complex nature of the threat hybrid analyzed by traditional methodologies can lead to vague predictions.

The concept of hybrid threat summarizes the relevant aspects of these constructions, combined with a pragmatic trend of operational art to sync all power tactical and operational planning actions to achieve strategic objectives.

Doctrine for Joint Operational planning focuses JP 5-0 sitting operational planning activities and provides decision makers the information needed to develop alternatives for OPLAN development. In turn, operational planning manual FM 5-0, addresses the planning and command-control exercise in full spectrum operations.

In 2011, the Center for Army Lessons Learned US study *Irregular Warfare: A SOF Perspective*, advancing the idea of cooperation and interoperability between conventional forces and special operations forces against opponents using specific tactics hybrid war[9].

Joint Vision 2020 is a document proclaiming the need for full spectrum dominance in battle, offering doctrinal answers to military threats of the XXI century. The document focuses on aspects of interoperability (technological, organizational and procedural), information superiority, decision-making and acting, can provide a starting point in addressing threats doctrinal / hybrid warfare.

Hybrid threats bring many challenges for military planners. Wide range of threats require the adoption of separate solutions for each challenge. Planning must address priority indirect measures of disruption and fractionation hybrid threat by introducing internal tensions or cancellation synergistic effect of component hybrid threat, instead of physical methods to counter the opponent's means and capabilities.

Defining and describing the threat in an operational ambiguous framework, flexibility in thinking, regular review of plans and decisions adapting to changes in operating environment, dynamic cooperation intra- and inter-organizational, preemptive analysis of the implications of military action in media plan (it should become a basic criteria in comparing different courses of action), systems integration and careful selection of military and non-military riposte to avoid unnecessary damage and suffering of the civilian population are the characteristics of future processes operational planning.

Analysis on strategic culture potential threats from nation states, transnational and regional groups can provide forecasts on future strategic behavior.

Hybride threats defy traditional preference for military campaign planners short, decisive, being continuous, diffuse, requiring a flexible and nuanced approach. Planning must also maintain the initiative in front of hybride threats than adopt response reactive solutions.

2.3 The need to respect LOAC

Military commanders are responsible for compliance with LOAC principles in armed conflict and the provisions of the 1949 Geneva Conventions on prisoners of war, wounded, sick and people refraining from hostilities.

The principle of military necessity requires forces to engage only in those necessary actions, in order to achieve a legitimate goal, attacks being strictly limited to military objectives. In addition to this, there is also the need to use military equipment in accordance with the laws of armed conficts, weapons systems that contravene international law being banned.

The principle of distinction requires the distinction between military and civilian targets, including a ban on the use of force on persons who refrain from military action. The

[9] ***, *Irregular Warfare: A SOF Perspective*, Center for Army Lessons Learned, Newsletter 11-34, Fort Leavenworth, Kansas, June 2011, p. 25, available at http://www.globalsecurity.org /military/library/report/ call/call_11-34.htm, accessed at 01.04.2015

central idea is to engage only valid military targets. This principle also requires opponents to locate military objectives outside civilian areas.

Proportionality principle refers to the gradual use of force in relation to the threat, to avoid excessive losses, while avoiding unnecessary suffering principle is based on the prohibition of the use weapons and methods of warfare of a nature to cause injury or unnecessary suffering.

Unconventional opponents - guerrillas, insurgents, terrorists and non-state armed groups - will exploit restrictions armed forces complying LOAC and principles of international humanitarian law by drawing them in populated areas of conflict, seeking to exploit the presence of civilians in those areas where conventional forces are forced to act restrictively. This strategy of deliberately putting civilians in distress, and aims to achieve by misinformation and propaganda, both attracting retaliatory actions against civilians in armed forces and international condemnation.

The *Edge Protective operation* in the Gaza (2014), IDF imposed a series of extraordinary methods to reduce losses among the civilian population: risk assessment airstrikes usability and mitigate these attacks, maximizing the use of guided munitions, explosives selecting acceptable yield, warning civilians through text messages, phone calls and radio transmissions of imminent attacks, even at the risk of surprise cancellation of the operation, which is a good faith commitment to meeting the LOAC. There have been numerous cases in which IDF, in these exceptional constraints, canceled missions fire on military targets valid if these missions showed an increased risk of collateral damage. IDF efforts to alleviate the suffering people of Gaza have been extended by sending food and medicine, medical evacuation missions, securing energy and re-commissioning of damaged infrastructure.

In a hybrid-type war, the military actions go, especially in densely populated areas and the opponent is positioned mainly in civilian targets, use of force is restricted, being necessary to take extra precautions to avoid civilian collateral damage. Warfare will be dots, led by army units mixed (regular forces and special operations forces) of low value, equipped with high-precision weapons, based on accurate and timely information on the position, nature, value, intention and ability of battle of the opponent. Regarding this, information structures will play a decisive role in the success of the operation. A review rules of engagement and possibly adopt additional restrictions on the use of combat power in highly-populated urban environments.

2.4 Remodeling force structures

Starting from the idea that hybrid threats are really effective against large organizations, bureaucratic, with hierarchies and rigid relational systems, it is necessary to rethink force structures to be redesigned modular, rapidly deployable and flexible, with a chain of simplified command and control, after the modeled of rapid reaction units, and having an integrated character (including the lower echelons) or joint environment capable of meeting all challenges of fighting, mostly urban.

The structure of forces acting in a hybrid conflict will be kept in a state of high efficiency, ready for deployment before the outbreak of the conflict. This rapid reaction force can be supported by an important conventional force, for the security of the area of operations.

It is important that in order to counter hybrid threats, a group of joint forces, combined, hybrid essentially, exists, with elements from all the structures involved (conventional forces, special forces, intelligence agencies, public order structures, specialized forces in countering cyber ACTIU , terrorist, psychological, electronic warfare, etc.) with a simplified control

system control, able to accelerate decision-making information flow to maintain the initiative at the strategic, operational and tactical.for,

Simultaneous use under a single command, of a main force and an irregular one, provides a synergistic advantage of pressure to the opponent, as the whole is greater than the sum of its parts. This approach differs from the Compund concept, the forces acting simultaneously in a single direction, but separately, with different degrees of coordination in battle.

To normalize the situation and support the indigenes, in a hybrid type war the forces involved must have the same type of combat operations, or as soon as the situation on the ground allows, to quickly deploy and support stability operations to restore security reconstruction and development of the essential elements of the economy, providing essential services to the population, support for local government and public order forces.

It is equally necessary to rethink the possibilities of equipping the forces, depending on the particular environment in which they operate and the level of threat. Opponents may adopt unconventional low-tech solutions to overcome technological advantages enjoyed by conventional armies to the same extent they can use advanced weapon systems. These technologies can be used simultaneously to create confusion and difficulties in planning and executing military operations.

There is a risk that the war expands in all environments, including, in addition to the three known environments (land, sea, aerian), the underground (tunnels for supply, omnidirectional and access to maneuver command and control facilities underground, whose efficiency was proved in the wars in Vietnam, Chechnya and Gaza Strip) or the underwater (use underwater fighters for attacks on critical objectives in coastal areas).

It requires that units operating in urban, densely populated are equipped with non-lethal weapon systems and research on how to use non-lethal technology in urban operations to be amplified.

However, further research is needed on the development and implementation of active protection systems, artillery launching point to detect, destroy projectiles (missiles) before impact, and launch facilities.

2.5 Adapting training and exercises to the new operational framework

Innovation and creativity are the lines of force in a hybrid war. A motivated enemy, free from any legal constraints, tactical and moral will seek to use the entire arsenal at its disposal in unexpected ways, unpredictable, maximizing losses among its forces. Urban guerrilla warfare tactics will experience improvements, adaptations and adjustments. The simultaneous and combined forms and procedures of the unconventional with conventional warfare, cyber attacks, terrorist and criminal, subversive and diffuse and the increase of "joint" of operations are the environmental characteristics of hybrid confrontation.

Source threat will be difficult to discern, real opponent mascându his intentions and actions by interposing paramilitary structures, non-military, separatist movements, pressure groups, state-pawn, or state-Trojan. The opponent can be incomprehensible, elusive and irrational.

Recent conflicts have shown that non-state actors is already operational concepts and military capabilities based on advanced technology, traditionally associated as belonging to national armies.

Therefore, we consider it necessary instruction and exercises are based on scenarios multinational joint applied urban areas by practicing the principles LOAC and managing relations with civil soceitatea. At national and multinational exercises, group commander of joint forces, and tactical commands can interact with decision makers (central public authorities / local), military and civilian structures with responsibility for security and image

vectors (the media NGOs, local leaders) of the area of operations. The armed forces must therefore have the ability to successfully operate in all environments, in complex conflicts.

2.6 Develop proactive capabilities on public information

In a real hybrid type conflict, war goes on communication channels and social networks, each party seeking to obtain public understanding about the legitimacy of its actions.

A state entity or organization, victim of a hybrid assault, must have efficient methods and techniques to counter misinformation and propaganda launched by the media, loss of information campaign with the magnitude of a defeat.

Denial, deceit, manipulation, intimidation and threats against the population and the media are tools used immediately and intensity of terrorist groups, non-state actors or undemocratic countries to manipulate the information to influence the public to question the legitimacy response actions from the international community, thus decreasing the will and motivation to fight from a legitimate military entities.

It is not enough that military forces engaged in operation to obey the laws of armed conflict, protect civilians, to use force in a proportionate manner, distinctive and according to military necessity. These legal measures should be made known to both internal and external public in real-time.

Military commanders must have the authority to convey, through their public relations structures (which must be active), public relations partner agencies, foreign ministry and diplomatic missions in national and international media, information interest in ongoing operations, based on relevant evidence (video and images) for their support. The messages will be adapted to target audiences, using all available information channels. Communication experts should be involved in strategic and operational planning where to analyse "media effect" of operations, including proactive response actions to misinformation from the opponent.

Equally, it must review the procedures regarding documents' transmission to media, since the operational planning products are classified. A balance between the need for public information and information security restrictions on the operations completed, ongoing and future should be corrected through a careful review of procedures.

Management and circulation of information of public interest will require a comprehensive, unified, coherent and concerted from all relevant stakeholders and communication vectors, civilian and military, with the support of civil society and benefit from new technologies, including analytical tools of social media.

Conclusions

The conflict nature has evolved rapidly in recent decades, from traditional, symmetrical to irregular, asymmetrical forms. Although asymmetrical threats are not new, recent conflicts have been marked by the use of innovative techniques and tactics, marking a dangerous development in the specter of war.

In future conflicts, conventional or asymmetrical actions will not be used exclusively, but a combination, as hybrid war. It incorporates a variety of capabilities, strategies and methods of waging battles, including conventional forces, formations and irregular tactics, terrorist and criminal disorder. The armed forces must therefore have the ability to successfully operate in all environments, in complex conflicts.

To counter hybrid-like threats, there is necessary to adopt an effective strategy response, based on a common doctrine and fundamental DGs.

A comprehensive approach is needed in all elements of power through cooperation, integration and strategic vision. Military actions will be part of a set of measures including political and diplomatic, economic, social, informational action.

Strengthening regional and global communication to ease geostrategic tensions and develop consultation processes regarding the increase in confidence and security will ensure the main action for the coordination of joint efforts to counter the symmetric, asymmetric and hybrid threats.

Monitoring transfers of funds, modern military capabilities and advanced weapon systems to states or non-state actors, can allow a predictive evaluation of hybrid threats and avoid strategic surprise.

Starting a new security strategy, the military system must adapt its programs regarding military education, defense planning, equipping and training the forces for the threats and challenges of the XXI century.

It is also necessary to create command and control flexible structures, adaptable and capable of providing the conditions for success for the forces involved in the full spectrum of military operations, including the hybrid threats.

Military operations should be supported by public information campaigns to counter the intense propaganda and disinformation attempts, maintaining strategic initiative and international media, public confidence.

Addressing hybrid threats and transformation of the armed forces must correspond to the strategic directives of the North Atlantic Alliance and the European Union, within a broader process of reorientation of European and Euro-Atlantic security policies. A national solution to hybrid threats is not desirable, as regional risks and threats cause a common response, unitary for the entire european continent and the international community.

BIBLIOGRAPHY:

1. AARONSON, Michael, *NATO Countering the Hybrid Threat*, disponibil la adresa http://cco.dodlive.mil/files/2014/02/Prism_111-124_Aaronson-Diessen.pdf, accesat la 01.04.2015
2. BOND, Margaret, *Hybrid war: a new paradigm for stability operations in failing states*, available at http://www.dtic.mil/dtic/tr/fulltext/u2/a468398.pdf, accessed at 25.03.2015
3. CASEY, George, *America's Army in an Era of Persistent Conflict*, Army Magazine (October 2008), available at http://www.ausa.org/publications/armymagazine /archive/2008/10/Documents/Casey_1008.pdf, accessed at 01.04.2015
4. DUŢU, Petre, *Asymmetric Threats or hybrid threats*, Publisher National Defence University "Carol I", Bucharest, 2013, available at http://cssas.unap.ro/ro /pdf_studii/amenintari_asimetrice_sau_amenintari_hibride.pdf, accessed at 01.04.2015
5. HOFFMAN, Frank ,*Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies, 2007, pp. 29
6. HUOVINEN,Petri, *Hybrid warfare–Just a Twist of Compound Warfare*, available at https://www.doria.fi/bitstream/handle/10024/74215/E4081_HuovinenKPO_EUK63.pdf, accessed at 01.04.2015

7. Johnson, David E., *Military Capabilities for Hybrid War. Insights from the Israel Defense Forces in Lebanon and Gaza*, available at http://www.rand.org/content/dam/rand /pubs/occasional_papers/2010/RAND_OP285.pdf, accessed at 20.03.2015
8. McCUEN, John , *Hybrid Wars*, available at http://www.au.af.mil/au/awc/ awcgate/milreview/mccuen08marapr.pdf, accessed at 01.04.2015
9. RUSSELL, Glenn, *Evolution and Conflict*, available at https://www.doria.fi/bitstream/handle/10024/92639/Y2622_HuovinenKPO_YEK56.pdf, accessed at 01.04.2015
10. WEITZ, Richard, *Countering Russia's Hybrid Threats*, available at http://www.diplomaatia.ee/en/article/countering-russias-hybrid-threats/, accessed at 01.04.2015
11. ***, *FM 5-0 The operations process,* available at https://fas.org/ irp/doddir/army/fm5-0.pdf, accessed at 01.04.2015
12. ***, IMSM-0292-2010, *Hybrid threats description and context*, 2010, available at http://cco.dodlive.mil/files/2014/02/Prism_111-124_Aaronson-Diessen.pdf, accessed at 01.04.2015
13. *** *Irregular Warfare: A SOF Perspective*, Center for Army Lessons Learned, Newsletter 11-34, Fort Leavenworth - Kansas, June 2011, p. 25, available at http://www.globalsecurity.org /military/library/report/call/call_11-34.htm, accessed at 01.04.2015
14. ***, JP 5-0 Joint Operation Planning, 2011, available at http://fas.org /irp/doddir/dod/jp5_0.pdf, accessed at 01.04.2015
15. ***, Ministry of Defence UK, *Future Character of Conflict Paper (FCOC),* available at adresa *https://www.gov.uk/government/uploads/system/uploads/attachment_data /file/33685/FCOCReadactedFinalWeb.pdf,* accessed at 23.03.2015
16. http://indianstrategicknowledgeonline.com/web/DIRIWCSCBriefv3.pdf, accessed at 01.04.2015
17. http://www.jinsa.org/files/2014GazaAssessmentReport.pdf, accessed at 20.03.2015
18. https://info.publicintelligence.net/USASOC-CounterUnconventionalWarfare.pdf, accessed at 20.03.2015
19. http://fas.org/irp/doddir/army/fm3-0.pdf, accessed at 20.03.2015
20. https://fas.org/irp/doddir/army/fm3-05-130.pdf, accessed at 20.03.2015
21. http://fas.org/irp/doddir/army/fm3-24fd.pdf, accessed at 20.03.2015
22. http://www.nato.int/cps/en/natolive/topics_69482.htm, accessed at 20.03.2015
23. http://www.aco.nato.int/page134134653.aspx, accessed at 20.03.2015
24. http://en.wikipedia.org/wiki/Hybrid_warfare, accessed at 20.03.2015
25. http://smallwarsjournal.com/blog/training-a-hybrid-warrior-at-the-infantry-officer-course, accessed at 20.03.2015
26. http://cgsc.contentdm.oclc.org/cdm/singleitem/collection/p4013coll3/id/2752/rec/1 , accessed at 20.03.2015
27. http://www.govexec.com/magazine/features/2008/05/hybrid-wars/26799/, accessed at 20.03.2015
28. http://www.nato.int/docu/review/2014/Also-in-2014/Deterring-hybrid-warfare/EN/index.htm, accessed at 20.03.2015
29. https://info.publicintelligence.net/USJFCOM-IrregularThreats.pdf, accessed at 20.03.2015

30. http://www.defenceiq.com/air-land-and-sea-defence-services/articles/the-21st-century-hybrid-threat-part-terrorist-part/, accessed at 20.03.2015
31. http://www.warcouncil.org/blog/2015/1/18/dynamic-doctrine-for-hybrid-threats-and-the-four-killer-es, accessed at 20.03.2015
32. http://www.ndc.nato.int/news/current_news.php?icode=758, accessed at 20.03.2015
33. http://www.globalsecurity.org/military/library/report/call/call_11-34_ch4.htm, accessed at 20.03.2015
34. http://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/, accessed at 20.03.2015
35. http://smallwarsjournal.com/jrnl/art/review-essay-fighting-and-learning-against-hybrid-threats, accessed at 20.03.2015
36. http://smallwarsjournal.com/jrnl/art/review-essay-history-and-hybrid-warfare, accessed at 20.03.2015
37. https://www.eda.europa.eu/info-hub/news/2015/01/26/increased-cooperation-to-counter-hybrid-threats, accessed at 20.03.2015
38. http://www.act.nato.int/act-countering-hybrid-threats-task-force-identifies-future-challenges, accessed at 20.03.2015
39. http://www.act.nato.int/the-countering-hybrid-threats-concept-development-experiment, accessed at 20.03.2015
40. http://iripaz.org/listado_docs/res_conflictos/Hofmann%20Naturaleza%20evolutiva%20del%20conflicto.pdf, accessed at 20.03.2015
41. http://www.armedforcesjournal.com/hybrid-vs-compound-war/. accessed at 20.03.2015
42. http://www.defenseone.com/ideas/2014/10/why-us-needs-strategy-counter-hybrid-warfare/97259/, accessed at 20.03.2015
43. http://www.specialforcestraining.info/topics/hybrid-warfare.htm, accessed at 20.03.2015
44. http://www.dtic.mil/whs/directives/corres/pdf/300007p.pdf, accessed at 20.03.2015
45. https://www.doria.fi/bitstream/handle/10024/74215/E4081_HuovinenKPO_EUK63.pdf?sequence=1, accessed at 20.03.2015
46. http://jsou.socom.mil/JSOU%20Publications/JSOU%2013-4_McCulloh, Johnson_Hybrid%20Warfare_final.pdf, accessed at 20.03.2015
47. http://www.fraw.org.uk/files/peace/us_dod_2000.pdf, accessed at 23.03.2015
48. http://www.defense.gov/news/newsarticle.aspx?id=45289, accessed at 23.03.2015

IMPROVING PERFORMANCE IN INTELLIGENCE – AN EXPERIMENTAL APROACH

Răzvan ŢUREA
PhD. Student at "MIHAI VITEAZUL" National Intelligence Academy, Bucharest,
e-mail: razvan.turea@yahoo.com

Abstract: *Generaly, there is a close link between human performance and awareness, as a part of emotional and social inteligence. Awareness implies a connection to the memory and attention as cognitive elements, a way to improve human performance is by training them. Increased skills based on memory and attention can increase performance, including the performance which is tied to the intelligence activity. For this matter, I have found a set of four technics which smoothens the level of awareness of the subjects. The experimental design used was a factorial one using two factors, applied in two levels. The experimental batch was made out of twenty-four students from the psychology department at the University of Bucharest, with ages from eighteen to twenty-three. Studying the difference between applied technics by applying the MANOVA test. For the study of the variables I have shown that there exists a semnificative difference between these technics, fact which allowed the identification of the most eficient techinique so that I could improve performance.*

Keywords: *intelligence, human performance, awareness, memory, atention, Kirilian effect.*

Introduction

Human performance has been defined starting from the concept of "performance" (as in mental performance, sporting performance etc.), using this meaning, being a individual capacity as a human being, to adapt and overcome unusual challenges. These challenges refer to the ones which overcome the normal parameters of a human being, being developed in the course of evolution.

Exceeding these skills can be determined by several factors; a reaction to the extreme weather, elevated stress etc. or even an intention such as a sporting event or cultural activities. Some of the human performances can be evaluated, trained and in doing so enhanced. Sometimes improving a certain type of performance we can obtain effects which also unexpectedly improve the performance in another field, without a direct link.

The training of multiple abilities can be direct towards a precise goal. This process is used to attain new levels of performance. This is also true for the intelligence activity. Today the intelligence activity has become, more than ever before, one fought on a mental battlefield. In this background, performance in the activity of intelligence is tied to the mental performances of the fighters in this theater of war. "The mind is an instrument of dealing with problems, depositing, extracting and processing information such as mental images which are present in the memory and which are processed by it"[1]. As a consequence there is a strong link between mental performances and some psychic processes such as attention and memory.

Through the smoothening of these processes using some methods and proper techniques, we can obtain enhanced performance in terms of awareness, which will empower and accelerate the transformation process of an intelligence activity to the standards which are

[1]http://www.dezvoltarium.ro/detalii- articol/legatura_dintre_creier_ si_constientizare, accesat la 20 iunie, 2013

stated in "the need for change"[2]. In the experimental survey that I conducted, I wanted to evaluate the act of awareness versus the human performance in intelligence activities. Two specifical skilss which a good agent should posess, are the ones of memory and attention. The defining characteristic of this experiment is given by the fact that the level of awareness, which was observed by applying the items on the Scale of awareness evaluation (CQ-I) is stable. The modification of this scale needs serious manipulative interventions, energetic ones and psiho-emotional ones. So, that I have piled up the items by applying the CQ-I scale, with the parameters which are specific to the human quantum field (HQF), in the dinamic of the adaptation mechanism for the enviroment needs, including the socio-profesional one. In this context, the evaluation of a technique, or a summum of techniques which can activate on their own if applied with the purpose of increasing performances in the intelligence domain, piled up with the act of awareness which can be done even indirectly through diffrent psihometrical instruments.

Because using the CQ-I scale to validate an interventional model on human subjects, would necesitate time intervals the size of years, I have divided the research into two stages. In the first moment, I have evaluated the subjects using the CQ-I scale and i have obtained numeral values of the characteristical items. In the pretesting condition I have measured the personal parameters using the GDV aparatus (Gas Discharge Visualisation) and the AV5.1 (Aura Vision). Following this I have evaluated the link between the CQ-I items of awareness and the psihoemotional parameters measured. In this stage I have used the FVW test to highlight the initial performances of the subjects which were part of the survey, looking out for attention and memory.

In the second stage of experimental research, the subjects did a set of specific techniques which followed the increase of own performances. After doing these procedures i have redone the measurings with the same aparatus and I have applied the same psihometrical instrument to obtain the values of the dependent variables.

With the help of the statistical test „*t student*" which applies to the paired groups for dependable variables with normaly distributed values, and with the help of the Wilcoxon test which applies dependent variables with values which do not respect the normal distribution, I have evaluated statisticaly the effects of specific techniques used to activate human skills.

1. Experiment description

The purpose experimental study

The purpose of this research was to find the link between awareness through its components memory and attention and the performances of the human being, in general and especialy in the activity of *intelligence.*

Objectives

Objective nr.1: The experimental demonstration of a link between the values of the parameters from the Human quantum field and the values of the items from the CQ-I test.

Objective nr.2: The experimental demonstration of a link between values of the parameters from the human quantum field and the visual and auditive memory.

Objective nr.3: Demonstrating the eficacity of the techniques used for activating own skills by applying some specific tehniques, using evaluating methodes for the human quantum field.

[2]Lucian Ion PETRAŞ, *Relaţionarea cu beneficiarii de intelligence în noua paradigmă - de la tirania hârtiei spre libertatea din wiki*, Intelligence, nr. 26, 2014, p. 120.

Objective nr.4: Experimental demonstration of the fact that there is a sinergical efect obtained by the sujects which have made the specifical training by mixing several tehniques, and this is semnificately bigger than the effect of applying a single tehnique.

Objective nr.5: Identifying, interpretating and determining a specific way of action to enhance specific parameters of the human quantum field, which are necessary for intelligence agents so that they could develop certain psihic skills.

Research hypotheses

Assumption nr.1: Subjects which record low values of the parameters from the human quantum field measured with the GDV and AV5.1 aparatus, show a lower lever of awareness, determined by applying the CQ-I test.

Assumption nr.2: Subjects which record low values of the CQ-I test, show a lower level of attention, visual and auditive memory.

Assumption nr.3: Subjects whose own skill were activated through the applying of specific tehniques, record a semnificative growth in the level of attention, visaul and auditive memory.

Assumption nr.4: Subjects , whose skills were activated through applying specific techniques, record an increase in the human quantum field using the GDV and AV5.1 aparatus.

Assumption nr.5 The synergistic efect obtained by the subjects who have done the specific training with combining more tehniques, is significantly higher than the effect of applying only one tehnique.

2. Method

Participants

The dimension of the experimental group was setted at a number of twenty-four subjects, divided in four groups of six.

The group was applied the procedure of parameter optimization for the human quantum field through specific skill activation.

Aparatus and instruments

The method used was the electrophysical research of states and energy[3]. This allows the visualisation and analisys by computerized recording of optical radiation and human biological emissions stimulated by the electromagnetical field and amplified by a gas leak[4], picking up the data using dermal sensors for the description of the human quantum field. The sistem allowed that the data to be processed and interpreted via the statistical program SPSS.

All the measuring described would be done automatically for each subject. In what concerns the effects which occur after the experimental sessions I will use the following clues:

- Changes in the biological and optical emissions stimulated by the electromagnetical fields and by a gas discharge, using the Kirlian effect;
- Changes of the parameters in the Human quantum field highlighted by the Aura Vision aparatus.

[3]Aliodor MANOLEA *„Condiţionarea psihosomatică. Psihodiagnoză şi intervenţie psihoterapeutică folosind stările modificate de conştiinţă”*, Universitatea Bucureşti, Scoala doctorală de Psihologie şi Ştiinţe ale Educaţiei, Departamentul Psihologie, Teza de doctorat, 2012, p. 116.

[4]K.onstantin, KOROTKOV, *Human energy field: study with GDV bioelectrography*, Fair Lawn, NJ, Backbone Publishing, 2002.

For highlighting the mentioned effects I have used GDV(Gas Discharge Visualisation), an aparatus which caracterizes the psihoemotional state and the somatic state of the subject included in the experimental group when it is being used according to the design of the experiment

The GDV (Gas Discharge Visualisation) method for measuring the biofotonic emision[5] offers the posibility of seeing and studying the emotional, psihical and phisical states of the human by determining a set of 42 dependable variables.

The results obtained are processed with the help of special programes which offer information regarding the psihoemotional and phisiological state of the subject undergoing investigation. The parameters of the images obtained by a gas leak, depend on the properties of the reasearched object and in this way analizing the character of the luminescence induced by objects who appear able to make valuable judgments regarding the energy state of the object in a specific time (Figure 1) .The analysis program is designed to process multiple static and dynamic parameters of diagrams and comparing the calculated statistical parameters to one or more of the samples being carried out by applying the Student criterion , the Wilcoxon criterion , Mann - Whitney criterion and Valde - Volfovitz , as well as sign criterion . A meta-analysis[6] of international scientific research conducted using the GDV and have been published in journals between 2003-2012 , estimates that :

-there are significant correlations between parameters measured with GDV and various medical parameters, physiological and psychological, thus validating apparatus and method;

-software and equipment EPC/GDV is a viable device, easy to use and offers a wide range of applications and methods of psycho- physiological assessment.

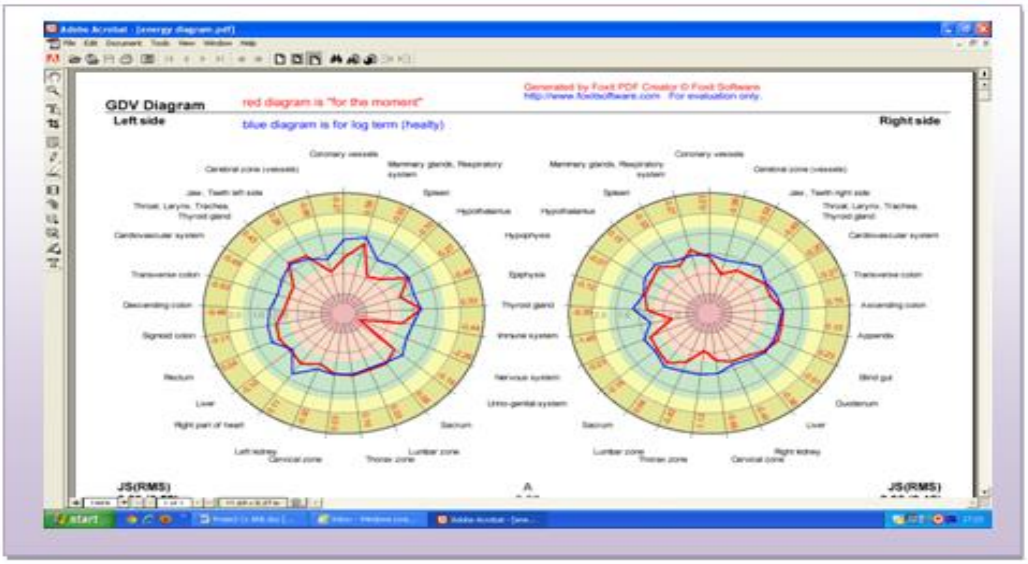


Figure no.1 Graphic highlighting of the human quantum parameters using GDV apparatus

[5] *Ibidem.*

[6] Konstantin G. KOROTKOV, P. MATRAVERS, D.V. ORLOV, *Application of Electrophotonic Capturing (EPC) Analysis Based on Gas Discharge Visualization (GDV) Technique in Medicine: a Systematic Review,* Journal of Altern Complement Med., 2010.

2.2.1 Metoda de evidenţiere a câmpului cuantic uman cu Aura Vision 5.1[7]

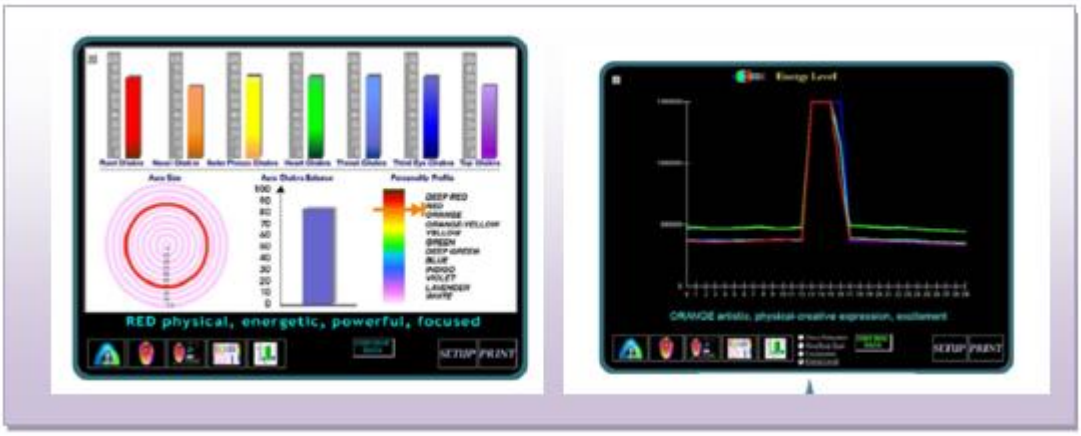


Figure no. 2 Graphic parameters recorded with AV5.1

The AV5.1 device is based on the interpretation of information of electro dermal activity and thermal emission ,at a palmar level . Processing this information with a specific informatical system provides information about mind-body - spirit balance , stress level , the level and quality of HQF 's principal quantum centers and in them about the functioning of the endocrine glands associated . Also elaborated and various information about the personality of the subject investigated (Figure 2).

Psihometrical instruments used

Awareness Rating Scale - CQ -I

The scale was developed from the assumption that there is a current level/current awareness reflecting the evolution of the person present in the wake state under normal conditions . The six dimensions of conscious experience[8] that were taken into account in assessing awareness, and which have become main factors for the Awareness Rating Scale are: Concrete awareness, Emotional Awareness , Mental Awareness , Spiritual Awareness and Social-rational Awareness. Awareness coefficient is obtained from the average of six main factors. The seven sub factors identified to describe the experience of other relevant facets awareness are internal state awareness , self- reflection , detachment , autonomy , personal development , positive relationships with others and purpose in life .

FVW test[9]

To assess attention and memory capacity for the FVW test, I used continuous visual recognition , which is part of the Vienna Test .

The respondent must decide whether an item is shown for the first time or repeated on the screen.

Working procedure

We used the test -retest manner of the FVW test for the performance evaluation of memory and attention, for each subject and CQ -I scale for determining the coefficients of awareness. All measurement values of the dependent variables were performed for each

[7]Aliodor MANOLEA, *Condiţionarea psihosomatică. Psihodiagnoză şi intervenţie psihoterapeutică folosind stările modificate de conştiinţă*, Universitatea Bucureşti, Scoala doctorală de Psihologie şi Ştiinţe ale Educaţiei, Departamentul Psihologie, Teza de doctorat, 2012, p.116.

[8]Ovidiu BRAZDĂU *Coeficientul de Conştientizare (CQ) The Consciousness Quotient & The CQ Inventory-Theory and Research,* Ed. Reţeaua Info-Sănătate, Bucureşti, 2011,pp. 110-125.

[9]Uli PUHR, *User manual for FVW Test*, Copyright for Test by Garching Instrumente G.m.b.H, Mödling, Austria, September 2003, pp. 3-4.

subject before and after activation of its potency by using breathing techniques and functional cognitions.

With regard to determining the effects before, during and after the experimental sessions (if applicable) I watched the different recorded values of variables in the experiment steps of:

-Quantum biological and optical emissions, stimulated electromagnetic fields by gas discharge using the Kirlian effect;

-The psihoenergetical state

- Human quantum field parameters;

-Affective emotional balance of the subjects in the experimental group;

Work stages

Phase I Sampling initial data from the batch

The experimental group performed the FVW test, applied CQ-I scale and quantum fields parameters were recorded for each subject.

Phase II of the application of the technique to activate their potencies of subjects participating in the experiment

At this stage breathing exercise and muscle contracture lower basin in four ways were made, each experimental group (of six subjects) addressing one way:

- Method A: exercise was accompanied by cognitive focus on mental count of times that steps corresponded to the subjects respiration.
- Method B: the exercise was accompanied by mental concentration on a linguistic structure with special spiritual significance.
- Method C: exercise was accompanied by moving the pelvis and cognitive focus on mental counts when the times coresponded with the stages of breathing.
- Method D: the exercise was accompanied by the moving of the pelvis and the mental concentration on a linguistical structure with a deep spiritual semnificance.

Experimental groups A, B, C and D have carried out this activity in a row, after the previous group had measurements of variable dependent values.

Phase III Sampling final research data.

With equipment there were recorded dependent variables as numerical parameter values, personal electrodermal and specific parameters of the quantum field. The whole experimental group was applied again FVW test for performance evaluation of memory and attention.

Stage IV Data analysis and interpretation

At this stage I used the set of programs Excel, SPSS 20, QPower for extracting statistical results.

Experimental design

The experimental design (figure 3) which was used, was one in a factorial plane with two factors, applied in two levels, resulting a factorial plan of a 2x2 type. The independent variables (factors) were breathing technique (with muscle contracture of the lower pelvis (RMBI) and moving the whole pelvis(RMBI - RB)) , and how to apply (with mental concentration on counting (CMNum) and mental concentration on structural elements with special spiritual semantic (CMSEss))

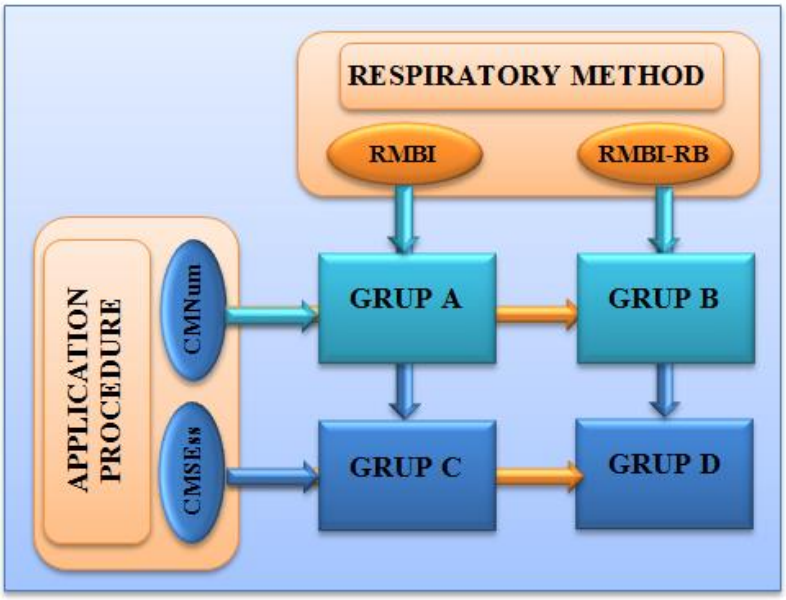


Figure no. 3 Experimental design- factorial plane 2x2

. Arrangements, shown in parentheses, represent the levels where the factors are applicable. Hence the name of 2x2 factorial planes, a plane is studied experimentally in two independent variables, each with two levels. Thus, in this experiment there are summarized in fact, four unifactorial experiments.

3. Discutions

Correlation analysis of test items CQ-I and dependent variables measured with GDV, AV5.1 show that it is possible to use these tools and tests to make an assessment of the current status of awareness of a subject, even if awareness is a quality of a human being, which varies relatively slowly. It was, moreover, the purpose of testing these two hypotheses. Correlation analysis of FVW test items and test items CQ-I, show that there is a link between skills measured with the FVW test, i.e. memory and attention and awareness as it is characterized by CQ-I test.

Applying a complex set of techniques for enhancing human performance (improving human quantum field parameters) I have shown that there is a statistically significant effect on the human being. This effect translates into a higher capacity memory and a more significant ability to keep attention focused on a target. This aspect was revealed by statistical testing of hypotheses three and four, which showed an increase in quantum field parameters correlated with a significant improvement in memory and attention.

Multivariate analysis techniques applied to increase human quantum field resulted in the fact that respiratory technique is crucial in obtaining the effect while the method of executing (counting with mental concentration (CMNum) and mental concentration on a structure special spiritual semantic elements (CMSEss)), does not have a statistically significant effect. This allows us to choose the method that is easier for subjects breathing and mental concentration pelvis moving on mental counting.

Conclusions

Without the presence of awareness, you probably did not know of the existence of our own perceptions. Realistically we know only a small part of them, one way of rising the focusing of attention, or mental concentration. "Awareness is like a screen showing all the

thoughts and feelings, and the mind becomes conscious of them by concentrating on them."[10]The mind solves problems, stores and retrieves information by concentrating on certain sensations, mental images and thoughts present in memory and processing them. Thus, there is a strong link between awareness and attention and memory skills. The relationship that we tested in this study, showing that there is a relatively strong correlation between test items CQ-I (awareness assessment questionnaire) and those of FVW test (test to assess memory performance and attention). It was necessary to do this because CQ-I test reveals changes, delays of awareness, and requiring long periods of time, of years, to reveal a change in the awareness of a subject. I needed a tool to highlight these changes in the structure of awareness in a very short time. The FVW test is suitable for this purpose. I also showed, that there is a strong correlation between test items CQ-I and dependent variables measured with GDV devices and AV5.1, being able to say that there is a strong correlation between human quantum field characteristics caused with these, and awareness of the subjects, as it results from the evaluation of CQ-I test.

I developed a set of techniques for activating human potential, that we have applied on subjects of the experiment and then, we tested their effect on the characteristics of the human quantum field caused by GDV and AV5.1 devices. Thus, we concluded that the techniques were effective, registering positive changes in human quantum field, coupled with improved performance and FVW test that measures memory and attention skills and their interaction. Therefore, I found a set of techniques that enable the human potential to improve the level of awareness of subjects who through increased skills related to memory and attention, can increase human performance including that related to intelligence activities. Studying the difference between the techniques applied by testing using analysis of MANOVA dependent variables, we showed that there is a difference between the independent variable in the breathing technique, while from the point of view of variable rules for the application, there was no one significant difference. This area involves Use the simplest ways to implement more effective breathing technique, namely breathing muscle contracture lower basin and basin with running mental count during respiration.

In conclusion, we have developed a tool for assessing and improving human performance technique consists of activating human potential (breathing muscle contracture and lower pelvis with mental count during respiration-RMBI_RB) whose effect is measured using GDV and AV5.1 equipment, and performance testing ,memory and attention test is evaluated with FVW.

BIBLIOGRAPHY:

1. ANITEI, Mihai, *Psihologie experimentală*, ed. Polirom, 2007.
2. BRAZDĂU, Ovidiu, *Coeficientul de Conştientizare (CQ) The Consciousness Quotient & The CQ Inventory-Theory and Research*, Ed. Reţeaua Info-Sănătate, Bucureşti, 2011
3. KOROTKOV, Konstantin, *Human energy field: study with GDV bioelectrography*, Fair Lawn, NJ, Backbone Publishing, 2002.
4. KOROTKOV, K.G., MATRAVERS, P., ORLOV, D.V., *Application of Electrophotonic Capturing (EPC) Analysis Based on Gas Discharge Visualization (GDV) Technique în Medicine: a Systematic Review.* J Altern Complement Med., 2010, 16(1).

[10] http://www.dezvoltarium.ro/detalii- articol/legatura_dintre_creier_ si_constientizare, accesat la 20 iunie, 2013

5. PETRAŞ Lucian Ion, *Relaţionarea cu beneficiarii de intelligence în noua paradigmă - de la tirania hârtiei spre libertatea din wiki*, Intelligence, nr. 26, 2014.
6. MANOLEA, Aliodor, *Condiţionarea psihosomatică. Psihodiagnoză şi intervenţie psihoterapeutică folosind stările modificate de conştiinţă*, Universitatea Bucureşti, Scoala doctorală de Psihologie şi Ştiinţe ale Educaţiei, Departamentul Psihologie, Teza de doctorat, 2012.
7. PUHR, Uli, *Manual for FVW Test*, Copyright for Test by Garching Instrumente G.m.b.H, Mödling, Austria, September 2003.

PERFORMANCE INCREASE IN THE ACTIVITY OF INTELLIGENCE THROUGH AWARENESS

Răzvan ŢUREA
PhD. Student at "MIHAI VITEAZUL" National Intelligence Academy, Bucharest,
e-mail: razvan.turea@yahoo.com

Abstract: *The final product in the work of intelligence, based on knowledge and objectivity, in accordance with the new paradigm of intelligence, is the result of efforts of the main pawn - the intelligence analyst. The quality of its reports is subject to specific training performance assimilated. Two dimensions of awareness, as a way to increase performance, they are important in this aspect, emotional intelligence and social intelligence. They are under new concepts in neuroscience, two sides of the human personality that can handle the specific methods involving the concept of neuroplasticity. It appears, surprisingly perhaps, a strong link between neuroscience methods and increase intelligence performance at all levels, from the point of view of the individual and the organization. In the evaluation of workers from intelligence we may use methods and practices of modern psychology, psychometric instruments appropriate to different aspects of personality-specific intelligence analyst performance.*

Keywords*: intelligence analyst , awareness , performance , emotional intelligence , neuroplasticity .*

Introduction

The world today is a conglomerate of companies strongly differentiated both socially, economically, politically, culturally, militarily, and informational. The globalization process determines, in addition to the positive effects of economic development and the progress of science, art and technology, and strong social disruption and in particular, military, leading, eventually, to conflicts of all kinds.

In the process of understanding and fighting the new theoretical models of conflict, leading to the concept of national security reconfiguration and create a new paradigm of security.

As part of this paradigm, intelligence missions were redesigned and reconfigured to meet the needs of providing security as a response to challenges increasingly complex and well designed, featuring most sophisticated resources, both material and human.

The human factor has not yet been outdated technology in the essence of the individual supervised / studied[1]. Human nature exceeds the level of technology, advanced technologies will be essential in the structure of the information.

On the battlefield of any kind may be, including the mentally, correct information should reach real-time fighter, he was forced by the dynamism of action to decide and act alone or with others. First, in this war of the mind[2], are agents, human intelligence sources that collect and verify the information of national security.

The next level, the formulation of intelligence analysis is provided intelligence analyst that "generate knowledge (primary analysis, structured comparison study of relevance,

[1] Stan PETRESCU**,** *Despre Intelligence, spionaj si contraspionaj*, Bucuresti, Editura Militară,. 2007
[2] *Ibidem.*

sorting, ranking, tinting, study of context etc.) confers attribute information strategic and organizes and summarizes the expert reports"[3].

1. Intelligence analyst, qualities and mental skills

A new trend[4], the theory of continuous change, sits in the center of the intelligence analysis cycle of intelligence gathering and directing both the production and dissemination of information (Figure 1).

Although seemingly simple, "it is a very complex refining process, which also means intelligence, critical thinking and creativity, intelligence analyst, and a very good knowledge of the area analyzed. Specifically, the analyst evaluates the information in terms of their relevance, detects changes and trends in the occurrence of threats, outlines alternative scenarios of evolution, highlights implications and indicates possible options in relation to each scenario forecast." [5]

In his work, the analyst has the duty to "overcome prejudice, to separate emotion information, rational impulse and strategical tactics"[6].

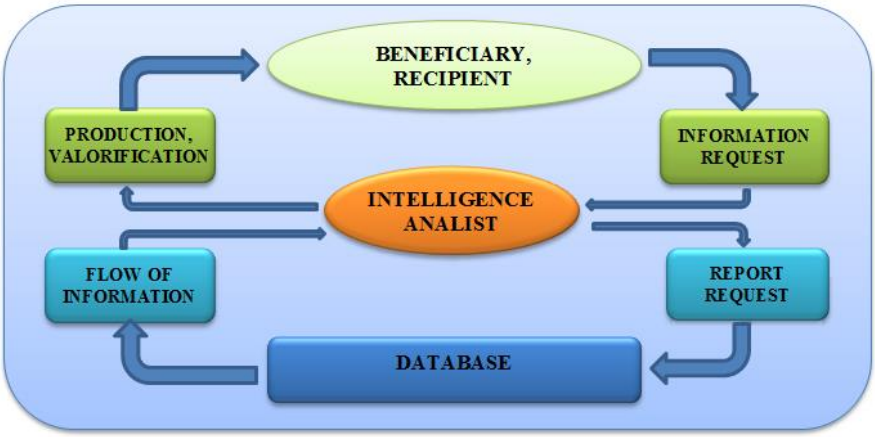


Figure no. 1 One analyst in the flow of intelligence .
(Source: Niţu Ionel , intelligence analyst Guide : handbook for junior analysts Publishing ANI MV, 2011 , p. 31)

Research on group decision making have shown, that they are dependent on the distribution of information within the group, while the information acquisition theory suggests that the intelligence analyst is a information avid, using coping strategies for achieving points objectively.

"Intelligence - as a theoretical discipline - has a low degree of conceptualizing and theorizing in relation to the other branches of social sciences. However, as Stephen Marrin[7]stressed, obtaining a level of abstraction that allows analysis of specific cases by refering to a rigorous conceptual framework is essential in order to answer questions such as: What types of organizational structures and processes analytical maximize product quality? What changes can be made to the structures and processes to improve this product? What best practices

[3] https://andreivocila.wordpress.com/2010/10/29/intelligence-ul-privat, accesat la 13 martie 2015
[4]Lucian Ion PETRAŞ, *Relaţionarea cu beneficiarii de intelligence în noua paradigmă - de la tirania hârtiei spre libertatea din wiki*, Intelligence, nr. 26, 2014, p. 119.
[5]http://www.sri.ro/analiza-intelligence.html, accesat la 12 sept. 2014.
[6] George Cristian MAIOR, *Incertitudine. Gandire strategica şi relaţii internaţionale în secolul XXI*, Bucureşti, Editura RAO, 2009, p. 36.
[7]Stephen MARRIN, , *Intelligence Studies Centers: Making Scholarship on Intelligence Analysis Useful*, în *Intelligence and National Security,* vol 27, nr. 3, 2012, pp. 398-422.

from other fields can be used to optimize the analytical process? What should I do to maximize performance analysts? What are the characteristics of intelligence analysts performing? "- George Maior said in the introduction to his work Ionel Nițu" intelligence analysis - an approach in terms of theories of change"[8]. The last two issues will be addressed in this paper, in order that best suits the theme explored.

Therefore, I seek to first answer the question, what are the characteristics of intelligence analysts performing? How the intelligence analyst thinks should be one as objective, neutral, to ensure the utmost quality of analysis, which is to describe reality as faithfully. Critical thinking[9] regarded as a cognitive and metacognitive act (the act of thinking observation, awareness of how problems are) at the same time can be a model to deal with. It is not enough to know critical thinking skills. A good analyst must have certain attitudes, rules, skills and traits of mind that using how to improve their critical thinking. Some empirical studies mentioned by Peter A. Facione and others indicate that it is necessary to achieve the intended purpose analyst, not only have critical thinking skills, and be willing to use them, which does not always happen.

There are some essential skills, mental attributes associated with critical thinking, as it states Faciones and Giancarlo[10] : the search for truth, openness to new approaches, unusual events, power analysis, systematic thinking, self-confidence, maturity of thought. On the other hand, Richard Paul and Gerald Nosich[11] states that "*the characteristics of critical thinking model can mention: independent thinking, self-centered and sociocentrismului understanding, intellectual modesty, the suspension of people and events, supporting ideas courage, loyalty and integrity, intellectual perseverance, confidence in reason, exploring feelings and emotions, intellectual curiosity* ". Both sets of skills are commonalities with the skills of an intelligence analyst as they were identified by David Moore and Lisa Krizan[12] i.e. permanent curiosity, fascination to identify events without fully knowing their motivation for continuing intellectual knowledge, insightful look in reality. All this helps to make surprising connections to solve the most difficult problems. Finally, emotional tensions created by these problems are obtained by finding the optimal solution. In addition, emotions, feelings and intuition play a significant role in critical thinking, as shown learning expert Stephen Brookfield[13]. He believes it is to find a different way of thinking than the commonly used analyst, one that requires creativity and intuition, qualities that are considered not to belong to rational thinking.

Skills and abilities listed are not characteristic only of intelligence analyst, they should characterize the vast majority of those working in this field. Ionel Nitu says[14] that, among those who collect information (agents) and those who process this information (analysts), there is a difference in communities cult classic information, and manages to demonstrate a sound scientific rationale, it was lower today, in this century, for several reasons. One is the need for change in order to meet new challenges in the field.

---

[8]http://www.ziaristionline.ro/2012/12/05/george-maior-despre-analiza-de-intelligence, accesat la 3 august 2013

[9]Peter A. FACIONE, Noreen C. FACIONE, Carol A .GIANCARLO, *The Disposition Toward Critical Thinking: Its Character, Measurement, and Relationship to Critical Thinking Skill*, Informal Logic 20, no. 1 2000, pp. 61–84.

[10]Peter A. FACIONE, Noreen C. FACIONE, Carol A .GIANCARLO, *Professional Judgment and the Disposition Toward Critical Thinking,* Milbrae, CA: California Academic Press, 2002.

[11]Richard W. PAUL, Gerald NOSICH, *Model for the National Assessment of Higher Order Thinking*, Dillon Beach, CA: Foundation for Critical Thinking, 2013, p.23.

[12]David MOORE, Lisa KRIZAN, *Intelligence Analysis: Does NSA Have What it Takes,* reprint NSA Center for Cryptologic History, Cryptologic Quarterly 20, nos. 1/2 , 2001, pp. 8–11.

[13]Stephen D. BROOKFIELD, *Developing Critical Thinkers: Challenging Adults to Explore Alternative Ways of Thinking and Acting,* San Francisco, CA: Jossey–Bass Publishers, 1987, p. 12.

[14]Lucian Ion PETRAȘ,*Relaționarea cu beneficiarii de intelligence în noua paradigmă - de la tirania hârtiei spre libertatea din wiki*, Intelligence, nr. 26, 2014, p. 120.

2. Human performance

The concept of human performance was defined based on the concept of "performance" specific (eg mental, sports, etc.) by a group of specialists in medicine, bio-motor skills and information theory. In this sense, human performance is the capacity of the individual, as a human being, to cope, to adapt to special conditions. Here, we refer to the special conditions exceeding "operational parameters "ordinary considered normal, which were developed during evolution and gene ontology.

Overcoming these facilities, skills, can take place under adverse conditions (eg. as a reaction to extreme environmental conditions, high stress, etc.) or can be made with a well-defined intent (performance sports, special mental activities, etc.). There are different aspects of human performance that can be assessed, trained and thus improved. By training specifically to a particular type of performance, we can obtain effects involving improved somewhat unexpected performance in another area, apparently without a direct link.
Interspecific training can be geared towards a specific purpose. This process is used to achieve new levels of performance and intelligence activities. In this context, business intelligence performance, improved methodologies and techniques as appropriate, would enhance and accelerate the transformation of intelligence worker, according to new trends indicated by the phrase "need for change"[15].

3. Consciousness, awareness

The etymology of the word (con- science, con- scientia, con-science) shows that a conscious organization is a reflection of science. It is a reflection of reality in which the human being, having provided sufficient information uses to understand and interpret a new object, phenomenon, event, occurred in the field of consciousness. " *From a psychological, man realizes, a " certain subjectivity and reproduces it in the form of images, notions, impressions"*[16]. By virtue of past experience, the object has echo information in the subject, in that it is realized almost right away.

Awareness, the observation of the act of thinking implies recognition of the individual in general and in particular the general retrieval. Also awareness plan implies a purpose in mind, as an essential element in conscious reflection. Goals being set before the activity, allow the individual to anticipate the outcome of his actions before their implementation in a concrete form. We find, in these few features of the process of awareness, some common points with the necessary skills and abilities as an intelligence analyst they were previously mentioned. In short, we can say that intelligence work requires individuals with high level of awareness, seen as an objective knowledge of reality (social, in our case).

4. Emotional intelligence and awareness

The concept of intelligence, assumed by some authors, a cognitive approach[17], which emphasizes mental abilities such as the ability to reason, plan, solve problems, abstract thinking, the understanding of complex ideas, to learning in general.

Intelligence cognitive, academic, was long considered a predictor of performance in areas pertaining to science, technology or in a broader sense, the work efficiency. But studies

[15] *Ibidem*, p. 121.
[16] http://www.aticmd.md/wp-content/uploads/2012/03/S_4_01_Todoroi.pdf
[17] Daniel GOLEMAN, *Inteligenţa emoţională*, editura Curtea Veche, 2008.

in the last two decades have shown that intelligence is not always correlated with cognitive performance[18], even in academic fields.

Situations where a person is judged not be classified in one perspective, as no one could say that individuals always have the same reactions to social stimuli. Aspects of affective, emotional began to be considered when talking of human knowledge and social environment that develops and operates. Emotional state of an individual determines how to interpret situations. Generate positive emotional disposition optimistic thinking, which causes high resolving problems, while negative emotions cause pessimism, blocking capacity for action and decision.

It would be wrong to deny the role of affectivity of feelings and emotions, where the purpose is social action toward effective relationship with the more so as these issues have a prominent role adaptive. Therefore opposition emotion - reason is inaccurate. Both cognitive processes (reason) and the affective (emotion) are inseparable in human action, even if they are different in operation and organization of mental forms[19]. A surprising aspect is aware that emotions and feelings seem to be indispensable to take rational decisions appropriate[20] to real social situations, decisions free from bias or emotional background of the individual.

Human behavior is very complex and is modulated by emotion, so sometimes we cannot accurately assess a person's reactions, even though we know it. Therefore, the ability to decipher, to perceive their own and others' emotions, to interpret and use to an end, is that not only provides social success. This ability has been called emotional intelligence and Daniel Goleman has considered a better predictor for social performance than cognitive intelligence, on the intellect. An individual with a high level of emotional intelligence can easily recognize and understand psycho-emotional behavior of other social partners. Developed Emotional intelligence involves innate skills as sensitivity (ability to recognize emotional structures manifested in subtle) emotional memory, high capacity processing both own emotions and social partners and last but not least, emotional learning ability, permanent. These features can undergo a process of improvement and development as and can degrade. At the same time, although high emotional intelligence is related to positive social behavior, it can be used to manipulate the behavior of social partners in their own interest [21].This is not necessarily an element of negativity, if we take into account the specific activity of intelligence.

On the other hand, there is a theory of multiple intelligence, or multifaceted, proposed by Howard Gardner[22]and summarized by Karl Albrecht acronym ASPEAK[23]:

Multiple intelligence categories		
Acronim	**Category**	**Description**
A	Abstract intelligence	Symbolic reasoning
S	Social intelligence	interaction with people
P	Practical intelligence	organization and tasks
E	Emotional intelligence	self-awareness and self-control

[18]*Ibidem,* p. 56.

[19] Mielu ZLATE, *Introducere In Psihologie*, Ed. Polirom, Bucureşti, 2007.

[20]Antonio DAMASIO, *Eroarea lui Descartes. Emoţiile,raţiunea şi creierul uman*, Ed. Humanitas,Bucureşti, 2005, p. 38.

[21]Y. NOZAKI, M. KOYASU, *The Relationship between Trait Emotional Intelligence and Interaction with Ostracized Others' Retaliation,* PLoS ONE 8(10): e77579. doi:10.1371/journal.pone.0077579, 2013.

[22]Howard GARDNER,.*Assessment of intellectual profiles: A perspective from multiple intelligences theory*. In D. Flanagan, C. Graham (Eds.), Contemporary intellectual assessment, New York, Guilford Press.2011, pp. 145-155.

[23]https://www.karlalbrecht.com/articles/pages/socialintelligence.htm, accesat 20 martie 2015.

A	Estetical intelligence	sense of form, design, and music, art
K	Kinestezical intelligence	skills related to physical mobility

Table no. 1 Aspects, multiple intelligence categories

These categories can be thought of as the faces of a cube, which is a whole that describes better human being. We note that this model is included and the social aspect of intelligence, a kind of awareness of a social strategy, combined with a set of skills to successfully interact in socially. In short, social intelligence as the ability to understand (relate) well with others and get them to cooperate with you.

Goleman, the original promoter of the idea of emotional intelligence with a broader in scope, which included both emotional and social, returned and acknowledged that a distinction must be made between the two issues [24]. An individual with a developed social intelligence can reduce the conflict, create conditions for good cooperation, replacing extremist behavior with a sympathetic attitude can mobilize people to achieve common goals.

There are many ambiguities concerning the definition of these concepts so that they can meet papers describing the concept of emotional intelligence using social consciousness characteristics and vice versa. Therefore, it is difficult to define which factors predict the existence and level of emotional intelligence and social.

After Bar-On [25] that is characteristic of emotional intelligence is the ability to acknowledge, understand and control their own emotions and process both and others in the social networking. He believes that emotional intelligence is an indicator of a person's general ability to adapt to difficult situations[26]**.**

5. What should we do to maximize analysts performance?

An agent in action, must always be connected to reality, to the present, aware so real events, undistorted by their emotions without their own apply a filter. This behavior ensures the objectivity of the analysis report. The intelligence worker must be an observer, as that allows him to objectively record the event as it unfolds, including all its aspects. Emotional[27] involvement and psycho-emotional conditiones and obscures certain aspects of events, reduced field of consciousness (Fig. 3), reducing the ability of intelligence worker to understand the whole context of the action, taking the best decisions.

[24]Daniel GOLEMAN, *Inteligenţa socială*, editura Curtea Veche, 2007.
[25]IuliaFODOR, *Inteligenta emotionala si stilurile de conducere*. Editura Lumen, 2009.
[26]Claudia DANILIUC, *Perspectivă asupra cercetării inteligenţei emoţionale şi sociale în relaţie cu dezvoltarea mentală*, Psihologia aplicată în structurile de apărare, ordine publică şi siguranţă naţională, între standardizare şi creativitate- *PSIHOPOL II*, 2010, p. 62.
[27]Aliodor MANOLEA, *Condiţionarea psihosomatică. Psihodiagnoză şi intervenţie psihoterapeutică folosind stările modificate de conştiinţă*, Universitatea Bucureşti, Scoala doctorală de Psihologie şi Ştiinţe ale Educaţiei, Departamentul Psihologie, Teza de doctorat, 2012, p. 69.

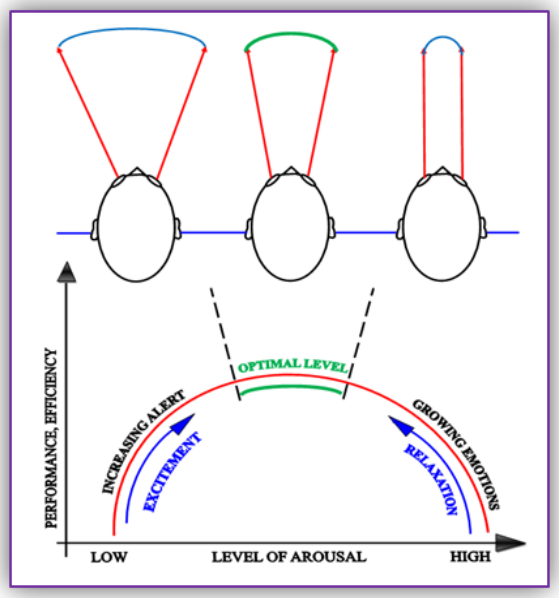


Figure no. 3 Conections arousal and field of consciousness with the efficiency and performance level

(Source: Manolea, A., Fundamentals epistemic, methodological and action on experimental investigation of the influence of distal psihoinformaţionale intelligence in action, "Challenges and strategies in public order and safety coordinators Mihai Badescu, Veronica Stoica, University Publishing House, Bucharest, 2014 pp. 493-499)

The ability to be an observer is one who can be trained, practiced and at the same time can be restored (if it was blocked by emotional conditioning) [28]**.** This capacity of observer, implies the existence of increased skills in the concentrated attention and memory, without which there can be no awareness of reality. These two processes can be considered precursors of psychic awareness. Improving poses a greater awareness of events social reality when it comes to intelligence activities.

Conclusions

As shown, the awareness is a very important feature of emotional and social intelligence, which is the ratio of proportionality with them. In other words, increased awareness lead the existence of a person with emotional and social intelligenc. These two aspects of human intelligence are directly correlated (positively) with the human performance in many areas of activity, including that of intelligence.

Correlation of performance in intelligence, with the two sides of human intelligence, result from coincidence of worker in intelligence characteristics, with those which define emotional and social intelligence.

Personnel selection for intelligence work should be done based, firstly, on the level of these two aspects of human intelligence using multiple assessment methods thereof. Then, those selected to be trained in the level of awareness that, as we have shown, increases the level of the two facets of intelligence. Methods that could be used, involve modification of certain behaviors by some techniques of modern psychology (cognitive-behavioral methods,

[28] *Ibidem.*

hypnosis, deep memory processes, psycho-quantum methods[29], etc.), methods whose results were highlighted by specific techniques of neuroscience.

They showed how neural networks are reconfigured during the application of psychological training methods [30]. Keeping the new configurations of these neural networks, through sustained training, causes permanent changes in behavior, so it is possible to improve, for example awareness, as knowledge of reality. Training memory and focused attention by specific methods, involving that certain neural network to keep their condition connected of for at least ten seconds, can be obtained raising awareness. This improvement in the level of awareness, can lead to the improvement of social and emotional intelligence, such as to achieve a significant increase of human performance, including in the activity of intelligence.

BIBLIOGRAPHY:

1. BROOKFIELD Stephen D., *Developing Critical Thinkers: Challenging Adults to Explore Alternative Ways of Thinking and Acting*, San Francisco, CA: Jossey–Bass Publishers, 1987.
2. DAMASIO Antonio, *Eroarea lui Descartes. Emoţiile,raţiunea şi creierul uman*, Ed. Humanitas,Bucureşti, 2005.
3. FACIONE Peter A., FACIONE Noreen C., GIANCARLO Carol A ., *Professional Judgment and the Disposition Toward Critical Thinking,* Milbrae, CA: California Academic Press, 2002.
4. FACIONE Peter A., FACIONE Noreen C., GIANCARLO Carol A., *The Disposition Toward Critical Thinking: Its Character, Measurement, and Relationship to Critical Thinking Skill*, Informal Logic 20, no. 1 2000.
5. GARDNER Howard,.*Assessment of intellectual profiles: A perspective from multiple intelligences theory*. In D. Flanagan, C. Graham (Eds.), Contemporary intellectual assessment, New York, Guilford Press.2011.
6. GOLEMAN Daniel, *Inteligenţa emoţională*, editura Curtea Veche, 2008.
7. GOLEMAN Daniel, *Inteligenţa socială*, editura Curtea Veche, 2007.
8. http://www.sri.ro/analiza-intelligence.html.
9. http://www.ziaristionline.ro/2012/12/05/george-maior-despre-analiza-de-intelligence.
10. MAIOR George Cristian, *Incertitudine. Gandire strategica şi relaţii internaţionale în secolul XXI*, Bucureşti, Editura RAO, 2009.
11. MANOLEA, Aliodor, *Condiţionarea psihosomatică. Psihodiagnoză şi intervenţie psihoterapeutică folosind stările modificate de conştiinţă*, Universitatea Bucureşti, Scoala doctorală de Psihologie şi Ştiinţe ale Educaţiei, Departamentul Psihologie, Teza de doctorat, 2012.
12. MARRIN Stephen, *Intelligence Studies Centers: Making Scholarship on Intelligence Analysis Useful*, în *Intelligence and National Security,* vol 27, nr. 3, 2012, pp. 398-422.

[29]Aliodor MANOLEA, Emphasizing the Psycho-quantum Way of Psychotherapeutic Action: Quantum Deep Psychotherapy. *Procedia-Social and Behavioral Sciences*, vol. 127, 2014, pp.636-639.

[30]B. ECKER, B. TOOMEY, () *Depotentiation of symptom-producing implicit memory în coherence therapy în Journal of Constructivist Psychology*, 21: DOI: 10.1080/10720530701853685, 2008, pp.87–150.

13. MOORE David, KRIZAN Lisa, *Intelligence Analysis: Does NSA Have What it Takes,* reprint NSA Center for Cryptologic History, Cryptologic Quarterly 20, nos. 1/2 , 2001.
14. NOZAKI Y., KOYASU M., *The Relationship between Trait Emotional Intelligence and Interaction with Ostracized Others' Retaliation,* PLoS ONE 8(10).
15. PAUL Richard W., NOSICH Gerald, *Model for the National Assessment of Higher Order Thinking*, Dillon Beach, CA: Foundation for Critical Thinking, 2013.
16. PETRAŞ Lucian Ion, *Relaţionarea cu beneficiarii de intelligence în noua paradigmă - de la tirania hârtiei spre libertatea din wiki*, Intelligence, nr. 26, 2014.
17. PETRESCU Stan**,** *Despre Intelligence, spionaj si contraspionaj*, Bucuresti, Editura Militară,. 2007.
18. ZLATE Mielu, *Introducere In Psihologie*, Ed. Polirom, Bucureşti, 2007.

MODERN INTELLIGENCE COMMUNITY IN KNOWLEDGE SOCIETY

Petrişor BĂDICĂ
PhD in "Intelligence and National Security", "MIHAI VITEAZUL" National Intelligence Academy, Bucharest, e-mail petrisor_35@yahoo.com

Abstract: *The dynamic security environment extends the specific need of structural and functional adaptation of CIM in a new paradigm anchored to the operational reality of the XXI century items of defense, national security, diplomacy, culture, economy, environment, etc. which are actively interpenetrated; the need for collaboration, integration, and innovation represent advanced knowledge and actionable solution for interconnection capabilities of entities informative.*

The current register of risks and threats specific to the modern security environment, characterized by high dynamics, variety, ambiguity and unevenness cause - effect, the Intelligence Community is structured and functions according to the intelligence parameters, where the Community represents the main provider of information required for info-decisions. It also ensures the info-decisions taken in the national security fields, by acting and developing a complex approach. The immediate effect of changing paradigm in domestic and international security is to transfer and share intelligence's role in info-decisions, where the political action is increasingly relying on the quality of intelligence.

Keywords*: the intelligence community, decision-making, informational revolution, Knowledge society, integrated system, sinergy and intelligence exchange*.

1. Modern intelligence community – theoretical and operational valences

In the context of current knowledge of the "intelligence" field, the concerns of defining and implementing the concept of "intelligence community" were developed especially among new democracies created after the Cold War, being closely linked to the need for an adequate response and to the risk factors uncertainty present in the operating environment of the XXI century that was marked by uncertainty, fragmentation, multiple connotations crises and threats activation of old and new forms of conflicts, among which we highlight confuntarea information.

Noteworthy became the obvious need for synergy in the national components of intelligence and participation in strategic decision-making processes allies (at NATO / EU) based on intelligence – all together with the national effort, and from this perspective, the action and the integrated place intelligence community into a new paradigm, organizational and functional, based on *modern principles and priorities*, among which we highlight on the *integration, collaboration, innovation*.

The values of the construction are related to new commitments, initiatives, anticipation and adaptability to complex challenges, collaboration, where one of its primary characteristics, is reliability[1].

[1] Karl Weick, the one that introduced the concept of high fiability organization, wrote in *1999: "The* high fiability organizations distinguish due to their own efforts to organize their manner in which quality is increased, developing also the people's alert level and awareness so that they can identify subtile and various contexts" (*Karl E. Weick and, Ted Putnam, Organizing for Mindfulness Eastern Wisdom and Western Knowledge* in Journal of Management Inquiry, Vol. 15 No. 3, , September 2006)

1.1. Theoretical considerations of modern intelligence community

The Community information is specific to each sovereign state, depending on its capacity and interests, (and its interests) being based on common principles of organization and functioning, but also of specific characteristics, given the objectives which they pursue, the means of achieving them, and printed character and process information. Lack of information equivalence of these communities is the expression of social rationality with which they were entitled.

In our view, currently, the intelligence community is an entity with major responsibilities for coordination, planning and management of information security necessary safeguard its values and interests of the nation, focusing mainly on multisource analytical evaluation and interpretation of information specific to this field and on the implementation of the general and operational strategies of national security.

The community information contributes to cover all areas of achieving national security, enable unified approach to managerial problems and functional structures that compose information involves avoiding duplication and overlap in the management of risks, threats and vulnerabilities that may affect the values of a nation .

The establishment of modern intelligence community (MIC) aimed primarily to fulfill its strategic mission[2]: *to create benefit decision making capabilities* by integrating external information, internal and military, technological and personnel policies, budgetary priorities and implementation plans.

This highlights a new paradigm in achieving the national security objectives and provides a challenge regarding the reform processes in the intelligence community of democratic states, where intelligence becomes constant social and dual relations between states without which the world modern can not function without them. "*... intelligence must be as efficient as it is flexible and smart to analyze, predict and forecast still obscure areas of knowledge*. [3]"

As expressed, the primary role of the IC is to provide strategic knowledge, concept developments where the information tends to dilute the consistency but can not be omitted because of the possibilities offered by new technologies for point targets, strategic.

Today, modern political decision is no longer taken in the absence of safety information derived from the IC, so intelligence failures or errors can be dramatic. "*A failure of intelligence activity is essentially incorrect understanding of a situation which causes a government (or its military forces) take inappropriate action or counterproductive in terms of his interests*[4]."

The main challenge of intelligence is inextricably linked to the role of the IC in the process of defining global security / regional / national reconfigurations and Member generating profound rethinking of objectives and missions institutions intelligence components and redefinition of relations of cooperation / collaboration the Allies, partnership or global information exchange. Here, we also aim the internal aspects related to the determination of the place and role of intelligence Services in the national intelligence architectures, tasks and responsibilities, strategies and objectives of reform or modernization.

Based on these coordinates, we assess that the primary objective and specificity of Modern Intelligence Community officials*, integrated and collaborative, is represented by the*

---

[2] ***, USA Intelligence Community Vision in 2015 - a global and integrated intelligence organization. Translated, Bucureşti, 2008.

[3] Maior, George-Cristian, "The intelligence Services and human's right is the era of the global terrrorism" in Steve Tsang (coord.), *"*The intelligence Services and human's right is the era of the global terrrorism – *The geopolitics of the XXI Century Worlds"*, Univers Enciclopedic, Bucureşti Publishing House, 2008, p. 10.

[4] N. Abraham Shulski şi J. Gary Schmitt, "The silent war – Introduction to the Secret Intelligence World"*,* Polirom Publishing House, Iaşi, 2008, p. 110.

level and relevance of strategic issues[5] related to political and diplomatic activities, economic, scientific and other guaranteeing the independence and national sovereignty, territorial integrity, constitutional order and its value system and unhindered in the promotion and implementation of fundamental interests of the international community, through actions conform to international law.

In the light of academic research, we can say that the definition of "*Community Information - organization of intelligence"* is one of the most important steps in shaping the efforts to reform the whole system of national security, a synergistic functional assembly and flow assurance challenges analytical products information necessary to support strategic decision.

1.2. Intelligence Community - organization of integrated, collaborative and innovative intelligence

In a modern vision, the company's future conflicts environment influences on strategic thinking will present the new features[6], will be governed by new principles[7] and will be supported by a diversified technological support.

The biggest threat of the XXI century, located at the border between conventional state of war and peace conventional state, mainly by non-state threats and vulnerabilities and new types of specific threats or use of cyberspace high technology and information technology, will increase a new type of confrontation specific to the knowledge society asymmetric network in a complex and dynamic multidimensional space (political, military, economic, diplomatic, informational, cybernetic, psychological, media, cosmic, cultural, etc.),based on the coordinates of ensuring control and domination of the information space and public communication or control / management activities / actions on these dimensions.

Reform trends identified during the study and deepen the organizational and functional intelligence communities in the Euro-Atlantic area and beyond, show that intelligence is considered an element of national power, and in this sense are accepted and those new skills in national legislation on the agenda for the new risks attributed generated intelligence or adapted their structural organization.

Through these challenges, the intelligence community is identifiable with the intelligence organization that has to response to higher needs of national security / Allied and needs that are related to the implementation of the four main objectives:

- the need to act jointly, due process of integration and globalization;
- working in joint teams (at inter-agency or multi-national) and research areas as large and deepening understanding of the mechanisms and phenomena of risk;
- the need for permanent recovery of information security by sharing knowledge;
- prioritization and selectivity security activities by generating joint projects, operational practices and adequate budgetary

In other words, in operational terms, we believe that MIC is an active construction, adaptable and integrated able to provide decision-benefit and modernize the following objectives[8]:

- *development of integrated intelligence capabilities* able to provide *strategic decisions* regarding new missions that are in the intelligence organization's loop (cyber defense,

[5] As component of the strategi leadership, according to Prof. Onişor Constantin, the strategic decision refer to all the activities conducted by the leadership system – foreseeing, planification, organizing, coordinating, controlling and ensuring the high-scale actions (Onişor Constantin, Bălan Mihail, Prună Cristian, *Intelligence and modern management strategic* Publishing House, Bucharest, 2012, p.34)

[6] New complex characteristics refer to misslaps concerning the technological developement, the influence on the hight-tech civilization, WMD threat, the internal responsability; the involvement in a new binominal type of terrorism-counterterrorism; impredictibility and flexibility.

[7] Noteworthy are higt-tech and I.T. principles and asimetric balances.

[8] These represent the main focus of USA'S IC in 2015.

interdependence and energy security, critical infrastructure protection, international peacekeeping operations - which requires intelligence support, proliferation of mass destruction, protecting scientific and technological innovation, financial disasters, economic competition, environmental issues, transnational threats and the hybrid use of nanotechnology, human rights violations, participation in managing the consequences of disasters, war criminals search, etc.)

- *creating a model for action in intelligence* that has the spotlight beneficiary national security information and that are based on the unity of purpose and objectives between it and the organization of intelligence by building networked with the players-beneficiaries analysts, managers and enabling recipients to discover, access and exploit security information safely and adjusted to individual needs, convinced that information products are strategic asset items that must be defended and promoted national interest or ally;
- *development of the "early warning" components* that are able to anticipate and prevent strategic surprises or provide opportunities for strategic decisions on preventing and combating security threats and risks;
- *intelligence community reconfiguration architecture* by integrating existing capabilities in the entities informative neural networks / collaborative platform able to provide easy work independently or in cooperation, in near real-time information on availability of stakeholders;
- generating unit operational doctrine in the community**;**
- *developing and improving interagency cooperation* framework in line with the security needs of the state and international commitments;
- *removing organizational barriers* that limit the internal and external collaboration by establishing a common practice in strategic planning, integrated analysis, mission management, dissemination of information, procurement policies, human resources management policies and training / training of staff, organizational security, exchange information, intelligence and adoption of legislation on relating to information security beneficiaries;
- *generation and imposing a new organizational culture* based on mutual trust, ideals and values, environment conducive to professional development in conditions of equality of opportunity, transparency and multilateral training, efficiency and effectiveness - in accordance with the performance standards set by the organization.

In consequence**,** the integrated intelligence organization must be built on a robust and dynamic information infrastructure based on a culture of sharing information and supported by a range of services and facilities to enable the user to turn the sheer volume final analytical data predictable information on which to act. Community information is identified as an organization capable of responding to threats and challenges of the knowledge society, has characteristics, an open and a great capacity for adaptability to environmental change, a robust organization, strong, with high levels of monitoring and control, with targeted activities agree with the following basic principles of operation of the system:

- *synergy - by integrating the separated elements of the system and ensuring impossible to achieve results if the units are autonomous and independent*;
- *flexibility - organizational capabilities are within the legal framework and the application of different methods that provide the primary endpoint: national security*;
- *efficiency - getting the most possible results with the available resources*
- *integrated work* as a team in an operational environment that fosters mutual trust, unity of effort and action, integration and transparency, adaptability and mental agility and proximity to beneficiaries' information products;

- *focusing on mission capabilities to achieve efficiency at all levels* (strategic, tactical, operational) including centralization of decentralization implementation planning, adaptive restructuring and redirecting resources on priorities;
- *providing expertise, capabilities, and enhancing strong partnerships* with academia, the private sector and international partners;
- *applicating performance management* to maximize individual work, team or organizational performance to ensure the beneficiaries of services and information products relevant to their needs, staff accountability for their actions and performance based on measurable results.

As shown, *obtaining the decisional advantage represents the MIC's strategic mission, and adaptability, is one of the conditions for the optimal functioning of its success*. Being constantly subject to transformations corresponding developments in the security environment, the development priorities of the intelligence community"*... are subsumed strategic goals whose achievement will ensure the premises to adapt to the challenges and opportunities of the information age 'operational capacity in the collection and recovery of information*[9] *; technology as a competitive advantage in intelligence; new perspectives on security services; investment in human resources; technology as a facilitator of cooperation; scientific research and technological development; institutional security; public communication in the information age*.

So MIC is identified and operates in a functional assemblies synergistic able to provide added value individual capacities and response processes multiplied and effective response to security risks and threats. *The intelligence community operates on the principles and logic integrated intelligence organization*.

2. Intelligence comunity reform - between needs and opportunities

In the current context of complex strategic development the objective is not to change its justification but rather "*...what kind of change must take an intelligence service, the manner in which this process can be interpreted as an opportunity, through a pro-active approach, in opposition with an passive, reactive interpretation*[10]".

In the specialists' opinion, modeling and building modern architecture intelligence is not exclusively related to the generation of large scale restructuring but directing future transformation of all actors involved in intelligence work, a new paradigm by:

- assimilating new technologies in operational activities;
- identifying mechanisms for effective use of information resources and the culture of information sharing;
- using much better the financial funds on projects of common security and operational priorities;
- developing a better coordiantion of the objective assessment of performance in the systematized and standardized context.

The performance degree of the integrated system[11] will be dependent on the implementation of new information and communication technologies and operational practices work for valuing integrated network, able to generate added value and operational vigilance intake with new threats and security challenges. This is represented by the necessary

---

[9] ***, - 2011-2015 Vision "*SRI in the informational era*"

[10] Maior George Cristian, Foreword in the *Ionel Niţu paper work –intelligence's analyze – an approch from the perspective of change's theories*, RAO Publishing House, 2012, pag. 13

[11] Onişor Constantin, *Performant Intelligence – gathering and analyzing information,*article, the scientific communication session organized by the National Intelligence Academy "Mihai Viteazul", 2011 – that can be found in the digital library of this institution.

efforts to ensure the freedom of the means of information, improve alertness information, reducing time intelligence for analysis appropriate, increasing accuracy by collecting information analysis, coordination and correlation component, rethinking the assessment processes of collecting information, defining the priorities, concentrating the operational efforts. All these should be achieved through inter / multi-agency teams, as well as growing quality support and technological component in current operations.

Transforming intelligence should be also analyzed from the perspective of joint IC's cooperation. Today it has become increasingly clear that the definition of national or regional security policies for the management of old and new threats risks is that "... *no intelligence Service can not be effective without a close cooperation with the domestic similar structures or foreign partners* ", meaning that efforts need to[12]:

- increase interconnectivity between intelligence to identify areas of interference and existing vulnerabilities boundary demarcation of several areas of knowledge in new areas on the agenda of their (critical infrastructure security, disruption of energy supplies, financial markets, climate change);
- build a robust information infrastructure based on the exploitation of new information technologies and a culture of information sharing;
- shift in emphasis from the "*exchange of information*" to "*knowledge exchange*" by addressing strategic knowledge exchange and management, operational capacity, robust networking, collaboration services permanent, integrated e-learning solutions, public viewing and systems organizational management;
- develop some virutual secure networks between Intelligence Community analysts and intelligence Services with access to databases made on issues or areas.

New technologies produce significant changes in the traditional missions of intelligence, sense the strengthening and development of a common IT infrastructure capable of supporting processes infodecizie, cooperation in internal format and connection networks, as well as quick and efficient query necessary data analysis processes information is assumed institutional objectives.

According to the American specialists there are two major changes in the environment to justify the need for the integration[13] of IC and creating strong opportunities for achieving integration[14]:

- today's missions are supported by the division between actors strategic or tactical level information (diplomatic, political, economic, military, etc.), but by integrating their efforts. Components are closely related to each other;
- information technology offers the opportunity for a closer and organic intelligence capabilities, characterized by unifying values rather than individual infrastructure traditionally associated with each discipline of information (Information Technology Infrastructure Management enables disparate evenly).

Based on this ground, the US's IC officials have acknowledged the need for a common consolidated and integrated. Integrating intelligence, may lead to new and collaborative processes capable of providing decision-support / beneficiaries possible because of new technology. The allegedly appered impediments, that are not insurmountable, can be addressed and overcome to achieve this integration.

---

[12] The adopted approach as per evaluating the problem in the article "Challenges concerning the definition of an intelligence national project" , published in the "Romanian magazine of Intelligence Studies" no. 8 / December 2012, National Intelligence Academy "Mihai Viteazul" Publishing House, Bucureşti, p. 74

[1313] The integrated Intelligence focuces on the strategic leadership of the state and contains all the decisions, planification and actions elements.

[14] AFCEA International, *National Security and Horizontal Integration,* USA, 2004.

Keeping outdated IC standards, reiterate the need that cultural development must take place in order to ensure the success of the reform process. New generations of officers are opened to innovative technologies, that represent the products of an information society, but as much are attracted the mysteries related to the intelligence activities. One of the challenges of this culture involves passing revolutionary usual "what needs to know" ("*need to know*") to individual *'liability offer*" (" *responsibility to provide* ") in order to work and help more those who need information.

Approaching cultural development in the IC requires / aims:

- to develop practical initiatives reforms line to produce effective performance in the community;
- to reset relations between intelligence between them and policymakers and military;
- to reduce the differences and organizational barriers - different cultures have interoperable systems, fuzzy decision rights and conflcituale business rules etc.;
- to strengthen the integrated information sources, challenge that comes to limit a new division between civil and military, internal and external.

Accessing a concept adapted to the modern intelligence in the knowledge society starts with the challenge launched by NATO over the fact that "*..together the elements of the system can be bettter achieved, than individually*" in a context dominated by the economic crisis and the desire NATO to streamline operations.

The concept of "*Smart Defence*", launched at the NATO Summit in Chicago in May 2012, the Alliance responds to the challenge of using limited resources with maximum efficiency, respect the principles of action puts the following: *prioritization of expenditure; specialization allies; cooperation among allies*.

We believe that the use of such a concept must be defined and applied to the architecture of national intelligence, given some undeniable facts: oversized structures, incoherence and competition for investments operational overlaps and generate much support structures than necessary skills not falling on the agenda of a modern intelligence service, launched concepts, meaningless and unapplied etc.

Amid "total war on terrorism" the investments made in the specialized force and in creating informational capabilities have increased exponentially, but economic realities and challenges of today induce a new way of thinking and acting in the intelligence community, based on serious analysis expenditure on national security / allied with the objective of keeping the IC returns and determination of significant reductions without compromising efficiency.

Human capital should be seen as a strategic resource to MIC and work on this line, the investment program in which decisions are based on the effectiveness of labor strategies and available resources, and the development of performance metrics, especially in developed areas exponentially in the community.

Another approach is system performance of staff. Essentially, this system can help improve MIC capacity, to also include reducing labor and rebalancing structures which have increased excessively in a situation at a time. These reductions must stand out so timely leaders could create incentives for preservation specialists in key areas and limiting their departure by private area. We must not forget that any reduction must be made according to the priorities assigned missions IC.

Given the annual increase in personnel costs in 1990 is increasingly likely that, amid the current crisis, budgets IC to flatten or even decrease. This requires labor maximizing the priorities assigned missions, maintaining the right level of support, maintenance technical expertise, challenges may appear in the staffing, procurement processes, recruitment, research and development domain dimensions of intelligence structures.

MIC must adapt to new fiscal realities and a strategy with a predetermined final plan and a plan for staff reductions is needed; but also maintaining the objectives and not damaging the basic capabilities of the organization. One challenge is with the young-experienced officers, although having developed capabilities tailored informational reality, they lack experience what may be a risk to the detriment of the mission.

Finally, IC must continue to develop labor efficiency through better use and fully exploiting integratelor OSINT capabilities (including the recruitment directed towards these sectors underused) strengthening partnerships with the private sector that can provide efficiency (areas of nanotechnology, software, hardware, high technology, etc.) and developing the exchange of information with foreign partners.

We can assess that budget cuts expected in the IC will induce a new kind of "intelligent" which can be seen at a possibility of rethinking / reset IC and leadership has to redefine tool, realign and refocus service missions information.

Conclusions

Current intelligence architectures are the result of geopolitical intelligence that falls between traditional approaches related to a certain historical period and trends reconfiguration of global power relations.The Community information in the XXI century responds to challenges and levels of security risks very complex, where their interconnection, is based on operational logic involving labor efficiency, strong partnerships with civil society and research centers / academic cooperation / collaboration through the exchange of information and knowledge nationally and internationally.

Based on the challenges of reform / transformation of the intelligence community, noteworthy would be to evaluate and to focus on several lines of research, among which:

- the study concept released in the research related to the approach “based on comprehensive network[15]” (multinodality) but also to the security and its implications for IC;
- creation of a national intelligence model in a project that includes internal, external and military intelligence services, along with protection structures and analysis departments created specifically identified risk areas such as financial and economic area, customs, etc., defining tasks and responsibilities for effective and integrated actions;
- defining institutional mechanisms for policy coordination to ensure optimum level of acceptability for adoption infodeciziei urgent issues on the agenda of intelligence;
- substantiation of performance evaluation procedures at individual, the intelligence and the whole community;
- develop a mechanism for "lessons learned" to boost components act of managing risk processes help to identify opportunities for organizational development and validation formulas provide individual and collective performance and to monitor progress.
- exploring and developing the concept that “people are the best resource intelligence organizations can have";
- definition of mechanisms for monitoring and control of organizational processes to ensure data change key parameters IC;

[15] This concept was launched by Felix Artega, Senior Analyst at Real Instituto Elcano de Estudios Internacionales y Estrategios/Spain. In the current context, new principles as pragmatism, flexibility and efficency, have to replace formalism, and the security problems are no longer framed by its national poles, and they can be better managed through various “actors” that activate at various levels.

- Innovation directed towards increasing technical and technological capacity (with effect collaborative formulas, standards and processes, common environment for operations, integrating security practices, improving integration and exchange of information, new technologies and modern procurement processes, etc.);

Noteworthy for MIC is that reform processes have led to a renewal of strategic thinking paradigm including a new division between military and civilian fields, internal and external, as well as greater integration of open source.

The final conclusion is that based on the current register of risks and threats, MIC is structured and functions as an intelligent organization of intelligence[16].

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. ***, - Vision 2011 -2015, SRI in the intelligence era, Bucharest;
2. Han Lawrence, *Intelligence and information management: global challenges and private information*, National Academy Press Information "Michael the Brave", Bucharest, 2011
3. Major, George-Cristian (eds.) - *A war of mind, intelligence, intelligence services and strategic knowledge in this century*, RAO Publishing House, Bucharest, 2010;
4. Major, George-Cristian, *Intelligence and human rights in the age of global terrorism* in Steve Tsang (eds.), "*Information Services and Human Rights in the age of global terrorism - XXI century geopolitics Worlds*" universe Encyclopedic Publishing House, Bucharest, 2008
5. Vision 2015 US Intelligence Community, Bucharest, 2008.

[16] According to Maior George Cristian as mentioned in the article "*Managing Change: The Romanian Intelligence Service în the 21 Century*", puiblished in "*International Journal of Intelligence and Counterintelligence" on 29.03.2012*, the concept of "*Smarter Intelligence*" aims to produce the following changes: to reorganize the missions and to make them more operational; to consolidate analytical system; to stress the training of a more trained and prepared HUMINT; to develop the technological compound; to increase the cooperation with internal and external partners; to deepen the relationship with the legal beneficiaries; as well as to cooperate with the reseach area in the academic and civil society.

SYNERGY IN INFORMATION SYSTEMS KNOWLEDGE SOCIETY. IMPLICATIONS FOR THE ORGANIZATION OF INTELLIGENCE

Petrişor BĂDICĂ, PhD
PhD in "Intelligence and National Security," "MIHAI VITEAZUL" National Intelligence Academy, Bucharest, e-mail petrisor_35@yahoo.com

Abstract: *Deepening knowledge and intelligent approach to the risk and threat phenomena specific to the current and future society, is facilitated by the adoption of new technologies as enablers of power factors, but also the design of modern architecture art intelligence and strategic parameters of valuing the organizational and functional synergy which is specific to the organization based on knowledge.*

In understanding and defining "functional synergy and action" of Modern Intelligence Community, achieved through the study of information systems in general, and of rationality and thought reform processes it should be regarded as a principle of modern information systems designed to bring additional value to actions / current operations and future, in terms of efficiency / effectiveness, proper allocation and use of resources needed to achieve them, as well as a high degree of satisfaction of beneficiaries of information products in relation to their expectations.

Synergy collection and analysis capabilities multidisciplinary threat environment is thus able to generate strategic vision for the adoption of security fundamental info-decisions, including the promotion and support of national interests / allies.

Keywords*: the intelligence community, decision-making, strategical awareness, informational revolution, capabilities, integrated system; sharing*.

Introduction

The motto of this scientific approach belongs to Albert Einstein and is as follows: "*The big issues we face can not be solved with the same level of thinking that created them*."

The pragmatic approach proposed title is based on the assumption of synergy's characteristics[1] as shown in the multitude of definitions developed on their reflection on the type of society in the current and projected future as well as interference with information systems for this type of company.

The radical change and the alarming threat environment is a reality of the XXI century, causing both corporate reassessment - economic, social life and policy approaches in a fluid paradigm where possible damage can be caused by weapons belonging this world (financial weapons, cyber - in all its forms, competition for natural resources, disease, etc.) and can be invisible, latent or progressive. The old "dilemmas" changes the meaning of knowledge, technological etymology, social dynamics and the transformation of intelligence reflects the need for change processes, techniques and analytical skills.

XXI century threats are interconnected, interdependent viral facility and which effects are amplified exponentially by new technologies, being aware that their manifestation sometimes exceeds our ability to understand the implications they have in terms of security

[1] Synergy can be described by the aphorism "one plus one equals three" and often explicit in terms of " multiplied energy " and "efficiency". The word comes from the Greek language, which consists of the word "sin" - translated as "by" or "with" and the word "ergon" - translated as "work" or "work". In literary translation, synergy is "working together" and defines enhanced effect that can be achieved by simultaneous action of several elements for a common goal.

and generate response strategies. Globalization and the information revolution have changed the analytical interest of the intelligence communities[2]. Unpredictable Fund is supported by the diversification of the types of security threats and expanding the area of their manifestations.

Current developments and future processes (reorganizing the modern intelligence structures starts from the reality that identifies new potential operational risk and threat amid mismatches current systems (political, economic, social, military, etc.), new facets of security (national, regional, global) spectrum features confrontation generated by modern information and the security challenges that go beyond traditional intelligence concerns. In fact, human society manifests itself as an integrated entity, appears as a single system that covers all over the world and where there no longer exists the ability of single movements, being pushed by a new law of interdependence, a connection that is part of an integrated system. In an interdependent world, the nation can not be isolated and must compete international security only to the extent that its shares are recognized as legitimate[3].

In these circumstances, the "*functional synergy and action*" must be regarded as a principle of modern information systems designed to bring added value to the system / intelligence operations, in terms of performance, being informational, and technico-operational supported and effectively coordinated by national bodies / Allied multidisciplinary yielding foundation timely decision info-winning national security and informational confrontation.

Given all the above-mentioned details, the principle of synergy and functionality determines the fuctionality of the intelligence organization – created in a network at national level, but also the developement of the necessary strategies to respond to emerging risks, atypical and transnational bi- or multilateral format, mainly NATO and EU partners or at selected clubs representation of intelligence.

1. The synergy of the intelligence systems in the knowledge society. multidisciplinary approach

Generating and implementing the modern informational systems, in a volatile environment which is connected to the nowdays evolutions (economic, sociale, political etc.), but also in an imprevisible and sensible environment, lead us to new insights of the society of knowledge, useful to the intelligence field, which can be defined and understood based on the sinergy created between the knowledge process and those connected to creativity, research and innovation. In this regard, the intellectual capital with its innovative and motivational valences, as well as the proper frame of knowledge – which contributes to the adequate valuing of all the actors involved in the national/international security – represents, from the modern intelligence perspective, the core of the society of knowledge. The stategical decisions rely on knowledge, and this detail comes to support the implematation of the security policies, as well as the welfare and the future of nation. Finding answers to the prospect of adapting to the demands of modern intelligence organization to the requrements of the environment of the intelligence confrontations, leads us inextricably to address three fundamental assumptions:

- foreseeing the place and role of the institution in terms of strategic objects parameters adapted to the needs of the information society and knowledge economy and community integrated social policy that protects and promotes

[2] W.J.Lahneman, *The Need for a New Intelligence Paradigm*, in International Journal of Intelligence and Counterintelligence, vol.23, 2010, p. 212.

[3] ***, White Paper on Defence and National Security of France, 2013 available on the Internet address http://fr.calameo.com/read/000331627d6f04ea4fe0e

- reforming the current context and conditions to ensure organizational performance, identified as a whole - organizational and operational and not as a sum of disparate institutions - something that involves implementing the principle of synergy, including the generation of a new organizational culture
- introducing the intelligence organization in a modern national gear called "national system for integrated management of crises" and a "national security community" with seats and defined roles for national institutions responsible, able to base national decisions in matters national security and contribute to the implementation of measures NATO / EU crisis response, according commitments.

1.1. The principle of synergy in the intelligence systems

The concept of system is in connection with the concept of synergy - seen as a result of combining subsystems and the resources of the system which, but also those which are identified as entire in excess "amount" possibilities parties separately. Whatever and however complex dynamic system operates and develops only due to its inner tensions which are maintained by the confrontation and the cooperation of the consisting components.

The synergy system, which is formed and developed through movement and organization, is also a result of the mutual interaction between strategy and organizational culture. Synergy means not only cooperation and / or competition subsystems, but also:

- *over-determination system to subsystems*, ie enslavement by the hierarchical system adjacent subsystems;
- *ordering the disorder* ("organized chaos" - H.Haken), which means the emergence of a displayed order (show) in involved order (hidden).

Based on all these reasons, the implementation of *the concept 2.0.*[4] affects the evolution of societies and organizations network, dynamic, adaptable and flexible, generating a new social architecture and a new philosophy of disseminating knowledge through collaboration to ensure collective knowledge.

This approach highlights the role of synergies in knowledge-based information systems[5], having as ground the detail that "... the intelligence society is defined as a the knowledge society and at the same time, as a society of organizations" (Drucker, 1992) and that their operation processes are determinant generic designated by the phrase "3I" and *innovation* (creation of new knowledge), *learning* (assimilation of new knowledge) and *partnership interactivity on knowledge*[6].

In this context, the development of the concept of synergy in the the intelligence system and the need for synergy in volatile and interconnected environment of the XXI century, are based on the assumption that the intelligence organizations based on knowledge area the main collective actors of the current society and have a role in its statement as being the society of knowlege from the following perspectives:

---

[4]The 2.0 Concept is solely connected to the Web evolution and to its applications used in all the social activities: management, inovations, education, international relations, strategic and political planification etc.

[5] The concept of knowledge organization has crystallized between the years 1984-1988, Huber (1984) appreciating the need for a new type of own organizational model succeeding the industrial society. The idea of knowledge organization can be found in two approaches that explain determinism, either from technological factors or from organizational factors. Promoters of information technology (Holsapple and Whinston -1987) define knowledge organization as a "community of workers with work design, interconnected by a computerized infrastructure". Managerial Approach (Drucker, 1988), deals with information based organization as the organizational model of the XXI century and its projected major Characteristic: dominant composition of professionals, small number of intermediate levels of the tree, ensuring coordination by means of non-authoritarian (standards, norms, rules of cooperation etc.).

[6] H.Dragomirescu, knowledge-based organizations, Thematic study developed under priority project "Information Society, Knowledge Society" of the Romanian Academy, Bucharest, 2001

- they belong to contemporan reality as professional and managerial work environment, object of scientific research and strategic project
- marks the convergence of two phenomena defining human nature (the knowledge and the organization), a flagship social construction ideas of collective competence, act smart and sustainable performance

Technological developments and current social dynamics, subordinated to the valences of a globalized world and interdependent intelligence require new attributes and responsibilities of Government, realizing that processes commonly used techniques and skills to be redefined and new operational concepts and validated to be borrowed from the private or the research / academic. Equally, unity of purpose and action for dealing XXI century security can not be achieved without unified action of all stakeholders who can provide knowledge, including the operation of theory / idea still invalid, but important assumptions made by processes of knowledge (eg . the concept of "knowmads[7]").

Under the impulse engines, the massive integration of advanced technologies in an integrated space confrontation will dominate objective of delivering systems involved, where the main challenges are posed by the degree of interoperability in information technology and the digitalisation of management, working hard to reach into formed a partnership in which cooperation is fundamental to achieving common goals.

Considering such identifying roles, missions and information flows in the areas of organization, its systemic approach represents the starting point in identifying and defining synergies. Intra- and interorganizational cooperation documents creates an information asset, characterized by intensity and fully dynamic parameters, we find complexity synergistic effects and synergy processes, the result of a principle derived "***cooperative competition***."

In the practic activity of the modern organization more frequently occurrs the positive synergies in the following six cases - without excluding other possibilities[8]:

- the coordination of the strategies' components of the organization;
- the integration of all capacities and capabilities by coordinating information flows, technical, logistics etc;
- the creation of new opportunities by combining existing potential;
- the addition of negotiating strength;
- the joint exploitation of tangible resources;
- the joint exploitation of know-how.

According to studies, the development of organizational and operational synergies will be addressed progressively support three behaviors:

- *redundancy* - "more organizations are acting like given the same objectives" - *which leads to*:
- *standardization* – "more organizations carrying on the same activities to achieve the same objectives" - *leads to:*
- *synergy* – "an organization engaged specific activities of several similar organizations and achieves more than could have been achieved if all these organizations would have conducted the same activity".

In substantiation of the expected responses, we reiterate the opportunity to exploit the concept of "*reengineering*[9]" in practice and organizational culture of intelligent organization.

---

[7] *The concept of* "*knowmads*" - identifies those nomadic knowledge workers (extension of the concept of "knowledge workers" launched by Peter Drucker in 1992 in vol. "Managing for the Future") and individuals creative, inventive and innovative that can work with anyone, anytime and anywhere.

[8] Radu Popescu, Synergetics in support of industrial companies achieve excellence in economic magazine no. 1/2004, pp. 25-27.

[9] The concept of *reengineering represents the fundamented rethinking nad radical reprojecting of the activities specific to the organization so that the results may be substantial in costs, quality and reaction speed* (Mihail Hammer)

Rethinking the organization's activities, including those with responsibilities in ensuring information security, joint action comes amid influences of objective factors of contemporary society on the whole process of knowledge (globalization, competition for high-level information - key resource, and even cyberspace conduct activities under virtual, electronic commerce, the existence of specialized personnel in data processing and analysis - knowledge worker, etc.) and necessary solutions can be generated / found and supported in the new ICT solutions.

1.2. Inter-sectoral synergies - fundamentals of performance information systems

Inter-sectoral synergies and interdependencies[10] idea in intelligence systems is a quantum transformation of mentality leading authority representing vertical level, intertwines with joint actions undertaken by the partners involved in achieving set goals, process in which a key role is played human factor .

Ensuring the integration synergies management within the operational areas are able to generate response strategies in line with rapid manifestation insecurity, and this can be translated as:

- *management business / mission* - exploit the full potential available (informational, human, technical, etc.) and provides a clear assignment of tasks;
- *inter-sectoral synergy*[11] - exploit its capabilities with those of partners / allies to increase overall efficiency.

So, from the perspective of an integrated information system are exploited three major perspectives:

- *building trust between community entities* - amid increasingly conduct of joint projects and stressed the need for unified action. Results are expected in terms of organizational autonomy, operational synergy and effectiveness of activities / operations;
- developing the ability of staff, translated by operational initiatives connected to the type and level of threat;
- *strengthening the role of management and establishing the authority activities / tasks* - amid need efficient use of available capabilities, establishing authority effort to generate operational synergies related to the allocation of resources on priorities and to synchronize actions, according to the type, threat level and speed of propagation. In other words, agility synergy management / control[12].

The challenges of such an approach in forecasting intelligence systems are related to:

- understanding a variety of approaches existing in the organizations performance of the related authorities and policies;
- developing clear guidelines and intent, including the evolution of the security environment;
- dynamic information environment and its impact on the activities / operations of intelligence, decisions taken and their real-time visibility in the international media;
- number, diversity and understanding capabilities and partner organizations participating in joint security projects;
- complexity and informational opportunities across borders for design and execution of intelligence operations, typically in the format ally.

---

[10] In fact, The interdependence is belongs to the inter-organizational environment and represents the trust between partnerts. Meanwhile, is also represents the awareness of the risks determined by the limited access to the development capabilities.

[11] The inter-sectorial synergy – according to Joint Operational Access Concept (JOAC 2012): The complementary vice merely additive employment of capabilities in different domains such that each enhances the effectiveness and compensates for the vulnerabilities of the others.

[12] It aims leading the integrated missions in the coooperation with the partners, as basis of the synuergy created between the operational fields.

In this context, cooperation and specialized inter-combining capacity can lead to effects beyond the belonging areas with relevance by increasing their effectiveness and organizational weaknesses in other areas. It is important that the results of synergies resulting amplify the results of tasks conducted in operational performance parameters.

Achieving synergies on cross-cutting challenges are:

- *recognition of reality and the need for interdependence* - no one will ensure the allocation of resources needed to fulfill the luxury / missions, which highlights the importance of interdependence / partnerships, "lessons learned" from operations, the idea of unified action and the ability to achieve the strategic goal;
- *gaining synergies and harmonizations*- with other national / allied or with other international partners, based on trust and decisions for solving together of critical tasks, just need amid the reaction unit interdependent risks. Although this area is needed to turn a dream into reality, yet are conscious efforts to ensure a high degree of understanding, cohesion, to alleviate the problems and risks based on personal relationships, use the connecting elements and decisions conscious dependence on partners for critical responsibilities.

The challenges posed by the new operational environment is reflected in the need to make further cross-sectoral synergies through[13]:

- knowledge of the operational environment and the need for interdependence;
- achieve synergy and confidence, especially with other systems and multinational entities;
- authority limits understanding, skills and capabilities of other participating systems (operational area, cyber, space, contra, etc.);
- valuing integrated practice management and coordination of actions of various systems;
- interoperability of systems and control systems;
- focus on unity of effort ..

2. Implementation of the synergy principle in the intelligence community

The developments in theory and practice specific to the organizational environment of the XXI century dominated by information and communication technology implementation in current activities, leads to the orientation of our research concerns to the model of "smart organization", flexible and competitive, and to identify factors facilitators of change in -a context of optimal match its structural projections - facilitating intelligent behavior, with the technology necessary to ensure competitive advantage.

The current organization is fully committed to implement new information technologies and value the power of information generated by network type actions - as the basis of modern organization and operation corresponding to the multiannual strategic vision to provide development opportunities and competitiveness in a dynamic competitive environment and new directives / principles to streamline networking: network consolidation; awareness and improve collaboration - with effects on the quality of information disseminated; auto-sync. This is reflected in an emancipation policy on access to information on all levels and by redefining the organization's internal and external relations.

A first hypothesis: the society of the future,the *smart organization concept* is redefined with the fundamentals change, synergy and leadership, a new way of thinking and performance through innovation and efficient use of their orientation directions of development, development

[13] Gary Luck (Gl.ret.) and the JS J7 Deployable Training Division (Martie 2013), *Mission Command and Cross - Domain Synergy*, accesibil pe Joint Staff J7 Joint Training Intelink (CAC enabled):https://intelshare.intelink.gov/sites/jcw/jt/default.aspx

and vision performance standards are met by groups / teams and 'communities of practice'. This thing can also be represented by the need of rapid adjustment of the organization to the transformations of the operational environment, the structures'operational flexibility, as well as efficient coordination - in top of all these has to be a performant management which promotes the prospective, conectivist and innovative approach of the risk and threat phenomenon - and of course also represented by the sinergy of all knowledge indicators in society, all together in cooperation processes (multidisciplinary, inter-disciplinary, specific expertise fields).

Flatten intermediate levels between leadership and members, involves the generation of a new model for intelligence institutions based on information. The role of information has become primordial communities after the events of 11 September 2001, particularly in environmental modeling, theory and practice of intelligence operative and profound implications extended to the global level. The *new intelligence community tends to become "knowledge provider"*.

We must not overlook the whole research approach is achieved in a context in which they are increasingly relevant knowledge provided P.Bobbit antinomies which are created by existing security models. Against this background, "*... the intelligence services face a world of uncertainty, the increasingly blurred borders and sinuous between war and peace, a world where failure can be a source of future success only if it is understood and processed as a need to change the way of thinking of analysts classic*[14]".

Applying modern concepts, among which we mention that of synergy, should generate strong ongoing structural changes in building construction intelligence of network organizations, more dynamic, flexible and competitive, specific requirements and challenges of the current environment security. The occurrence of specific resources developed within the intelligence ("-INT sites"), closely related to and conditioned by technological developments on the one hand, and the emergence of non-traditional and asymmetric risks, on the other hand, requires the importance of finding springs synergistic functionality for beams and modern information systems, intelligence institution specifically for operational performance advantage necessary to obtain the decision, in our opinion, its strategic mission.

The use of smart technology software and professional applications can increase processing capacity and refining useful information on building and strengthening networking and the establishment, strengthening and enhancement of competitive advantages due to interconnections with other similar systems whose functionality is based on competitive intelligence and cooperation. On these grounds, redefining the institution of intelligence sits synergistic perspective, as a prerequisite*, a number of objectives, among which*[15]*:*

- conceptual compatibility and actioning all togehter with the intelligence and security structures in the Euro-Atlantic area;
- clear separation of powers components of community structures, eliminating overlapping and duplication structural and operational;
- unified strategic analysis of information on national security;
- organizing processes of knowledge by developing a national strategy for intelligence;
- homogenized coordination of activities that are related to national security in areas of competence of the designated national authority structures, such as preventing and combating terrorism, CYBERINT areas, IMINT, GEOINT, SIGINT, PROTINT, OSINT - thus shortening cycle and thus promoting operational decision on behalf of the organization public-private partnerships;
- inducing the idea of creating a new organizational culture;

[14] P.Bobbitt, *Terror and Consent. The Wars for the Twenty-First Century*, Penguin Books, Londra, p.290

[15] Bădică P., Ştefan R.(2008), Challenges concerning the definition of a natioanl intelligence project, in the Romanian magazine of Intelligence Studies no. 8 / 2012, pp. 61-62.

- ensuring effective action and communication services aligned to energize components of the new organization of intelligence;
- increasing internal interoperability in web intelligence and eliminate unproductive competition between community structures;
- providing feed-back operational legal beneficiaries of intelligence products, improving cycle information and their involvement in defining an operational culture in this area;
- optimizating and coordinating Diplomacy's intelligence;
- operationalizing the Centres of Excellence in Intelligence and unifying the approach of training processes, training, research and exploitation of intelligence community;
- developing relationships with private structures of intelligence, especially in the area of risk analysis and promotion on behalf of legislation intelligence organization.

A new operational model must be *defined and operationalized in line with the 4 principles of intelligence* (*integrated management missions, gathering information adapted, combined analysis, strategic partnership*); to be centered on mission, agile, dynamic, flexible enough and have capable intelligence roles which have to adapt to the new challenges, to incorporate new technologies and processes to develop the areas of integration and collaboration with channel-day constraints or functional organizational laws.

Tackling such a complex model involving multiple analysis, meaning they are required to be analyzed results of a *study on the challenges facing the modern private companies, most competitive* (in the pharmaceutical, electronic, commercial, chemical), made in connection with the development process intelligence and knowledge management, *the main conclusions are*[16]*:*

- *intelligence mission has changed* - from a passive means of obtaining information, under the command of decision makers at an internal active agent (not determine the hierarchical position or product information needs at each subunit of an organization provides input necessary. Intelligence acquires the two dimensions: individual agent analyst is a personal network, the product is tailored to individuals and to the specific situation);
- *intelligence is dispersed*, there is both in the central structures of an organization, as well as in subsidiaries or project teams which, in turn, cooperate with similar groups, but based on common interests, not in coordination with central manager specially appointed;
- *traditional intelligence cycle* - planning is the prerogative of decision-makers, and other components (data collection, analysis, dissemination) are tasks of team work is conceptually correct, but describes the process of intelligence at a organizaţionals implificat not individual one complex;
- *practitioners are involved in activities other than those strictly related to the decision-making process such a*s: organizing / participating in "conversations" analytical; updating the standard; ordering information and profiling competitors;
- *intelligence is created to improve and support business decision making.*
- *In this regard*, it redefines the role of practitioners in the fields of knowledge initiation, reducing the time and cost needed to create knowledge, disseminating guidance initiatives within the organization and creation of knowledge.

On these lines, building synergistic organization will be guided by intelligence and knowledge of these challenges.

Enlightening the end of this research approach is the speech of John C. Gannon[17] who notes that "*... the merger's intelligence, people trained and synergy of advanced technologies*

[16] *Journal of Studies in Business* – Magnus Hope – *The Intelligence Worker as a Knowledge activist – an alternative view on intelligence by the use of Bukes pentad*/march 2013.

[17] *Ten Years After 9/11: Is Intelligence Reforme Working?*, Opening Statementof John C.Gannon to the US Senate Homeland Security and Government Affairs Committee Hearing, May 12, 2011, pp.1-6

and joint interagency teamwork are the highest ever achieved celmai .. . while it is always room for improvement in the work of intelligence, strong performance, our collaborative agencies ... today is unprecedented - and a source of pride for IC justified ".

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. ***, - Intelligence Overview of US Intelligence Community, SUA, 2011;
2. ***, - USA 2015 Strategy – A global and integrated intelligence organization, translated., Bucharest, 2008;
3. ***, 2011 – 2015 Strategy "SRI in the information age", Bucharest, 2011;
4. David S. Alberts (2002), *Information Age Transformation, DoD Command and Control Research Program* – accessed on the web address - http://www.dodccrp.org/files/ Alberts_IAT.pdf, in 10.02.2015
5. Fingar, Thomas, *Reducing Uncertainty: Intelligence and National Security. Using Intelligence to Anticipate Opportunities and Shape the Future*, Stanford University, October 2009
6. Lahneman, William J., *The Need for a New Intelligence Paradigm*, in "International Journal of Intelligence and CounterIntelligence", vol. 23, no. 2, 25 February 2010
7. Maior George Cristian, *Uncertainty, Strategic thinking and international relations in the XXIst Century*, Publishing House RAO Bucharest, 2009
8. Maior, George Cristian, (coord.), *The War of mind. Intelligence, intelligence services and strategic knowledge in the XXIst Century*, publishing house RAO, Bucharest, 2010;
9. Maior, George Cristian, Konoplyov Sergei (coord.) – *Strategic knowledge in the extended area of the Black Sea*, Publishing House RAO, Bucharest 2011;
10. Matei, Florina Cristiana, *Romania's Intelligence Comunity: From an Instrument of Dictatorship to Serving Democracy*, in International Journal of Intelligence and Counterintelligence, nr. 4/2007;
11. Mihaela, Muresan- *The synergy between knowledge, creativity, research, innovation and education* – accessed on the web address http://euromentor.ucdc.ro /dec2011/ro/sinergiadintrecunoasterecreativitatecercetaremihaelamuresan_9.pdf
12. Niţu, Ionel, *Intelligence analysis. The changing theories approach*., Publishing house RAO, Bucharest, 2012
13. Pallaris, Chris, *Open Source Intelligence:A Strategic Enabler of National Security*, CSS Analyses in Security Policy, vol.3, no.32, 2008

EXPERIMENTAL RESEARCH OF PSYCHO - INFORMATIONAL DISTAL INFLUENCE[1]

Aliodor MANOLEA, PhD
Doctor of Psychology (Ph.D.), University of Bucharest
Doctor of Science - Complementary Medicine (D.Sc.), The Open University for the Complementary Medicines, Colombo, SriLanka.
Ph.D. Candidate in Military Science, "CAROL I" National Defence University, Bucharest.
e-mail: aliodor@glide.ro

Abstract: *The experimental demonstration of the transmission of information, apparently without material support, in warfare operations, is possible by recording the EEG pattern of brain activity produced by exposure to the emotional visual stimuli between spatially and sensory isolated subjects. The phenomenon of brain connectivity, during what we called Distant Psycho -Informational Influence, is demonstrated by determining of the coherence of the signals and using the ERD / ERS neuroscientific classifier.*

Keywords: *psycho-informational, distal, subliminal, coherence, synchronization*.

The phrase Distal Psycho-informational Influence (IPsiD) is an integrating concept, which includes an extension of subliminal communication and influence in the kinetic domain of action[2]. The purpose of using distal psycho-informational influence, in all the steps of the warfare action, is to alter the psycho-emotional capacities of the enemy need to carry out combat operations, to diminish their capabilities to make decisions, at all levels, from the commanders to the troops, to weaken the enemy's determination to fight.

Structure of the Experiment

The experiment consisted in the simultaneous exposure of inductor subjects to visual stimuli with emotional signification and in measuring the effect of the supposed distal psycho-informational transmission to receptor subjects. The brain activity of both categories of subjects was monitored using wireless one-channel MindWave Mobile EEG headsets, which were conected with a data-acquisition system including three laptops, with time synchronizing covered through the internet. The operating system used was LINUX. The electrode of each EEG headset was placed in the prefrontal lobe area of each subject, in the Fp1 point in the placing scheme 10-20 of the EEG electrodes on the scalp. The master computer was running the PSYCHOPY[3] application, which managed the temporal unfolding of the experiment, concerning the exposure to visual stimuli with emotional contents. Visual stimuli were displayed simultaneously for all inducer subjects on displays M1...M8 by means

[1]A., Manolea, *Acţiunea beligenă şi influenţarea psihoinformaţională distală,* referat Scoala Doctorală Ştiinţe Militare şi Informaţii, UNAp, Bucureşti, pp.4-65.
[2]A., Manolea, *Influenţa psihoinformaţională distală ca parte a influenţei informaţionale de intelligence*. Academia Nationala de Informatii "Mihai Viteazul" International conference „Intelligence in the knowledge society" Bucharest, Romania, October 19th, 2012. Biblioteca electronica a Academiei Nationale de Informații (ANI), Colectia "ANI - Mihai Viteazul", ISBN 978-606-532-062-3.
[3]J.W., Peirce, *Generating stimuli for neuroscience using PsychoPy*. Frontiers in Neuroinform. 2:10. doi:10.3389/neuro. 11.010.2008.

of a video distributor (VS). On the appropriate displays, receptor subjects could see only black mark on the center of the screen.

Three experiments were carried out, unintentional and intentional, each on 16 inexperienced subjects (without specific psycho-informational training) and another intentional one on 16 subjects, of which eight subjects had particular psycho-informational training (activation of own potential by the neutral technique). On the whole there were 48 subjects participating to these experiments, of which 40 were students of the Faculty of Psychology of the Bucharest University and eight belonged to a group with specific psycho-informational training.

All three experiments were carried out during the same temporal timeframe. Each test included 25 sessions to which participated groups of subjects distributed using the Fibonacci sequence[4].

Each session of each trial included nine images, each with a duration of six seconds, preceded by a warning pause of 4 seconds, some with positive emotional contents, other with negative contents and other emotionally neutral.

The uneven number sessions (1, 3, 5... 25) had as inductors subjects from Room 1, and for the even number ones inductor subjects from Room 2. There were eight subjects in Room 1 and eight in Room 2, isolated spatially by a reinforced concrete wall.

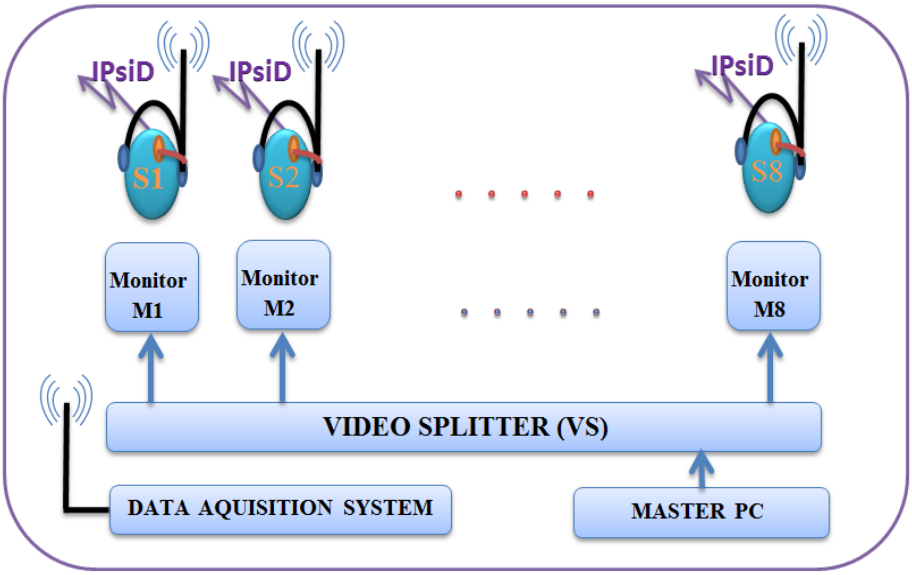


Figure no. 1 Experimental mounting for subjects in Room 1 (Manolea, A. 2014)

There were measured, synchronized in time, the brain activity of the inductor and receiver subjects, and have processed the obtained data using several application packages for the signals analysis: EXCEL, MATLAB, EEGLAB and ASAEEG, in order to extract the information packed in the EEG structure. All individual EEG channels have been reunited in a structure corresponding to the EEG 10-20 scheme, with a maximum of 19 channels, out of which only 15 channels were activated, because one channel of the data acquisition system did not work.

The EEG recording corresponding to each subject was assimilated to one channel, specific for the recording of one EEG with the 10-20 electrodes system.

[4] A., Manolea, *Fundamente epistemice ale influenţei psihoinformaţionale distale,* Buletinul UNAP nr.1/2013, pp. 378-382.

The correspondence was: S1-Fp1, S2-Fp2, S3-F7, S4-Fz, S5-F8, S6-T3, S7-Cz, S8-T4, S9-O1, S10-O2, S11-T5, S12-P3, S13-Pz, S14-P4, S15-T6 and S16-Oz, where S_i are the 16 subjects. In so doing, were able to use the analytical facilities of the EEG analysis program, which simultaneously process all the signals, so that the results were obtained in a unitary manner, by using the same processing procedures, with the same values for the specific parameters.

Thus, EEG electrodes corresponding to the front half of the model scalp corresponded with the EEG recordings of subjects in Room 1 and the ones of the back of the head corresponded to the EEG recordings of subjects in Room 2.

Methods for Studying the Synchronization of Brain Activity

The hypothesis behind any EEG analysis is that the certain patterns of brain activity always correspond to the same triggering events and the other way round, in other words that there is a bi-univocal relation between triggering events and the pattern of brain activity. In our case, the triggering events were the emotions generated by the exposure of inductor subjects to images with emotional contents, and the assumption was that by some mechanism, so far unexplained, these emotions are distally sent to other subjects, without them being in any whatsoever contact and without any awareness[5]. In fact the intention was to measure what happens, how and whether any information is sent from the inductor subjects to the receiver ones, when the intention is present and when it is not. At the data processing level, this fact is equivalent to the existence of common patterns of brain activity, both of inductor and receptor subjects.

This analysis is based on the supposition that brain activity is specific to each interaction of the human being with the environment, whatever it may be, or, in other words, adapted to our case, each emotion produces a particular pattern of brain activity. If we find similar structures in the time or frequency domains then we can say that there is a high degree of similarity between the events (emotions) that have caused that structure of brain activity in inductor subjects.

ERS/ERD–Event Related Synchronization/Event Related Desynchronization Method

A typical method to analyze EEG is the averaging of data in order to identify certain structures, patterns appearing at certain fixed moments in time, related to specific events (e.g. stimuli or responses to stimuli) – the so-called ERP's (Event Related Potential). By averaging, the signal-noise ratio is dramatically improved so that a certain characteristic structure becomes visible. However, in many cases (such as the present one), there are no well determined moments in time, related to the appearance of brain activity related to a certain event, because we do not know how and when an image with emotional contents causes an emotion in the mind of the inductor subject. The electrical activity of the brain of the inductor subject, produced by emotions, can be caused by his/her memories or some unconscious mechanism related to instinctive reactions like fight or flight, so there is a non-determination regarding the moment of arising of a pattern of the electrical activity of the brain (EEG).

The non-determination, about the moment of occurrence of the transmission of information, is specific for the distal psycho-informational influence (IPsiD). So if we use the

[5] [5]A., Manolea, *Fundamente epistemice ale influenţei psihoinformaţionale distale,* Buletinul UNAP nr.1/2013, pp. 378-382.

ERP determination method, the information will be destroyed by the averaging because it does not appear at the same intervals from the triggering event for all the sessions of the experiment. This fact can be avoided by applying the method of synchronization / desynchronization analysis (ERS / ERD – Event Related Synchronization / Event Related Desynchronization) to the brain activity determined by the occurrence of certain events at somehow random moments in time. ERS represents an increase in amplitude of the power of brain waves in a particular band of frequencies, of short duration and well localized spatially, whereas ERD represents a decrease of amplitude. These increases /decreases in amplitude are not correlated in phase with a certain event and are very specific for certain bands of frequency (alpha, beta, gamma, delta and theta), i.e. they can appear in certain bands of frequency but not in others. For this reason, the unprocessed EEG recordings look like a chaotic, random signal, which does not seem to contain very clear patterns of brain activity, unless in well known cases.

The calculation of ERS and ERD is used to get an image of the dynamics of neural networks, in our case of the dynamics of links between the brain activities of inductor and receptor subjects.

EEG Coherence Method

Another method used to show there is a similarity between two EEG signals is the calculation of the coherence between them. The coherence is similar to the temporal correlation between two signals, but it is an estimator of similarity (giving us an image of the coupling of signals) in the frequency range. Coherence can show us there are common patterns of brain activity in certain frequency bands, whereas the temporal correlation is masking these patterns. Coherence is a complex function, of which the amplitude varied between 0 and 1. Here zero shows a lack of similarity between signals and values close to 1 a high similarity.

Preliminary Results

We must not forget that the image of brain activity as shown here is a simulation of the brain activity of all the subjects in the experiment, each EEG signal corresponding to one subject. Thus, an image of the standard scalp contains up to 15 virtual electrodes corresponding to each subject. In the case of the uneven number sessions of the experiment, the group of electrodes Fp1, Fp2, F7, Fz, F8, T3, Cz and T4 represent inductor subjects, and the group of electrodes O1, O2, T5, P3, Pz, P4 and T6 receptor subjects, the roles being reversed for sessions with even number.

Testing of Hypothesis

Hypothesis no.1 *Highlighting the existence of temporal synchronization of brain activity models (patterns) common both to inductor and receptor subjects.*

The results presented further have been obtained using the application package for the interpretation of EEG records, EEGLAB[6], a project coordinated by Swartz Center for Computational Neuroscience (SCCN) of the Institute for Neural Computation of the University of California, San Diego.

In the figure no. 2 we note the variance of intensity of the connection between brain activities of two subjects during an experimental distal influencing session. The highest EEG

[6] A. Delorme, S. Makeig, „EEGLAB: an open source toolbox for analysis of single-trial EEG dynamics". *Journal of Neuroscience Methods* 134:9-21, 2004.

power, common to both subjects, is in the delta and theta (1-7,5Hz) frequency domain of brain waves. The theta frequency range characterizes the subconscious activity, the domain of subliminal perceptions.

Also, we note the rhythmic variation of the intensity of connection of brain activities of both subjects. A curve which shows for the most part a strong correlation (the maximums of the graph are in the intervals 10-20s, 30-40s, 60-70s, 70-80s, 80-90s) to the moment when images with emotional contents appear. Images with an emotional effect have appeared at 14s, 24s, 34s...94s, i.e. intervals of ten seconds, with the duration of six seconds. This fact was recorded in most of the experimental sessions with higher or lower frequency, depending on four factors. The first factor was the ability to focus and keep it for a sufficiently long time, to enable us to say that the power of brainwaves was sufficiently high to generate such effects. The second factor is related to the concentrated focus which a subject can show, a factor with a high variability especially when it has to be maintained for a long time, in our case nearly 100 seconds. In general, an untrained subject cannot keep his/her attention focused on only one mental objective for more than a few seconds. The third factor is the training that the participating subjects have undergone. Of the 48 participating subjects, only eight have had a specific training for the improvement of their capacity to maintain attention and focus, the others being classified in the normality profile. The fourth factor was the activation of the own potential using the neutral technique, an activation which is part of the training program, of which the same eight subjects have benefited.

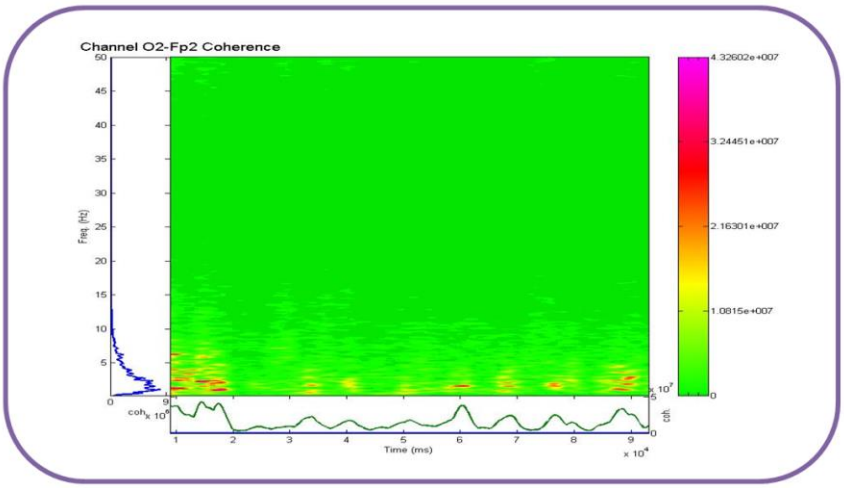


Figure no. 2 Interaction between the brain activities of two subjects (S2 and S10) represented in the frequency domain (left graph) from and in the time domain (lower graph). The graph in the center shows the connection of the two subjects both in frequency and in time (Manolea, A. 2014)

Also, if we study the connection between the subjects by using the method of ERS/ERD assessment (figure no. 3) we note, this time on a global scale (for all the subjects at once), how alternations occur between the coupling (ERS synchronization) and decoupling moments (ERD desynchronization).

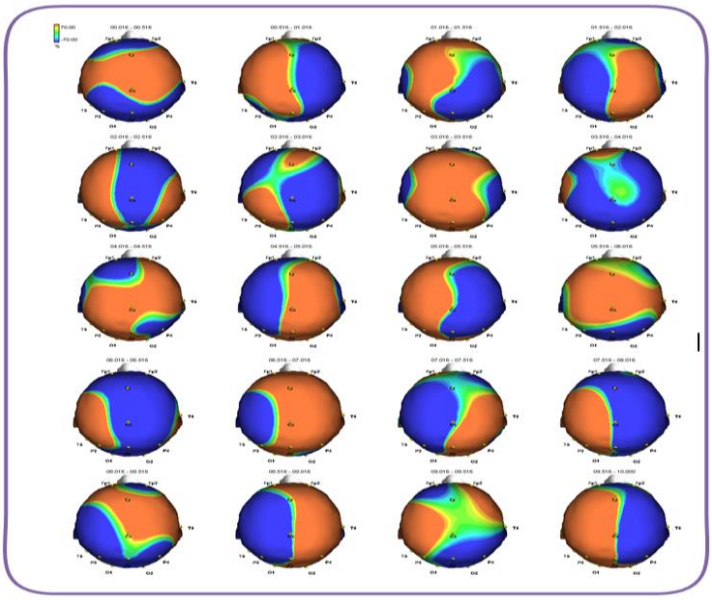


Figure no. 3 Dynamics of ERD/ERS (synchronization - desynchronization of brain activity) in the interval of 10-20 seconds (every 0.5 s) of the experimental session and the theta range (2-4 Hz). The synchronization of the brain activity is rendered in red and the desynchronization in blue EEG electrodes positioning on the scalp, according to system 10-20 (Manolea, A. 2014)

The moments of synchronization correspond to an increase in power of brain waves, and the desynchronization ones to a decrease of this power[7]. We also note how various subjects become connected (synchronized) on turns or together, this being a feature highlighted by this type of analysis[8]. Thus, we can say that the subject can be related to more subjects. We note there are short intervals (less than 0.5 seconds) when the brain activity of the involved subjects takes a break, becomes desynchronized, detached. The neural networks of the receptor subject show a maximum of availability[9] to the distal influence.

Therefore, the influencing action seems to occur in impulses. In fact that a higher power can be available only for short periods of time, among others also due to the possibility of subjects to maintain their attention and focus fixed for a longer or shorter interval.

We can thus say that there is rhythmic temporal relationship between the patterns of brain activity of the subjects participating to this experiment.

Hypothesis no.2 *The subjects whose own power was activated were less influenced than the ones who did not go through such a process.*

Another modality to show the connectivity between two systems is to highlight the coherent function. This function serves to estimate the correlation between two systems in the frequency domain. Images shown further indicate the amplitude of coherence between all the 15 subjects participating to the two experimental sessions of the type eight inductors and seven receptors, changing roles on turn.

[7] Durka, P. J., Zygierewicz, J., Klekowicz, H., Ginter, J., Blinowska, K. J."On the statistical significance of event-related EEG desynchronization and synchronization in the time-frequency plane". *Biomedical Engineering, IEEE Transactions*, 51(7), 2004, pp.1167-1175.

[8] O., Brazdău, „Constiinta si misterele fizicii cuantice", *Buletinul psihologiei transpersonale*, Numărul 7-8/2003, http://www.arpt.ro/RO/TPBuletin/7-8-2003.htm, accesat 11.11.2012.

[9] G., Pfurtscheller, F.H., Lopes da Silva „Event-related EEG/MEG synchronization and desynchronization: basic principles". *Clinical neurophysiology*, Vol. 110, No. 11. (November 1999), pp. 1842-1857.

The eight subjects in room one, were those who had benefited from a training program and who benefited from the activation of their own powers by the neutral technique. What do we note?

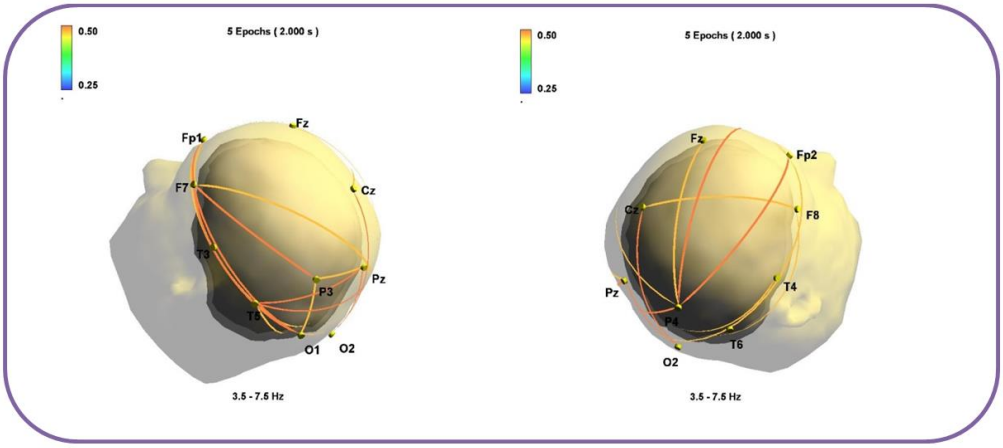


Figure no. 4 Amplitude of coherence (interval 0.25 - 0.50) for the session where the trained subjects were the inductors (12 connections with the receptors)
(Manolea, A. 2014)

In figure 4 we see that trained inductors managed to establish 12 connections with the 7 receptor subjects, links with a value of coherence in the interval 0.25 - 0.5, a significant value[10], considering this concerns different brains.

From figure 5, it results that the subjects with no specific training were able to establish only five connections with the receptors, which shows us they had a lower efficiency.

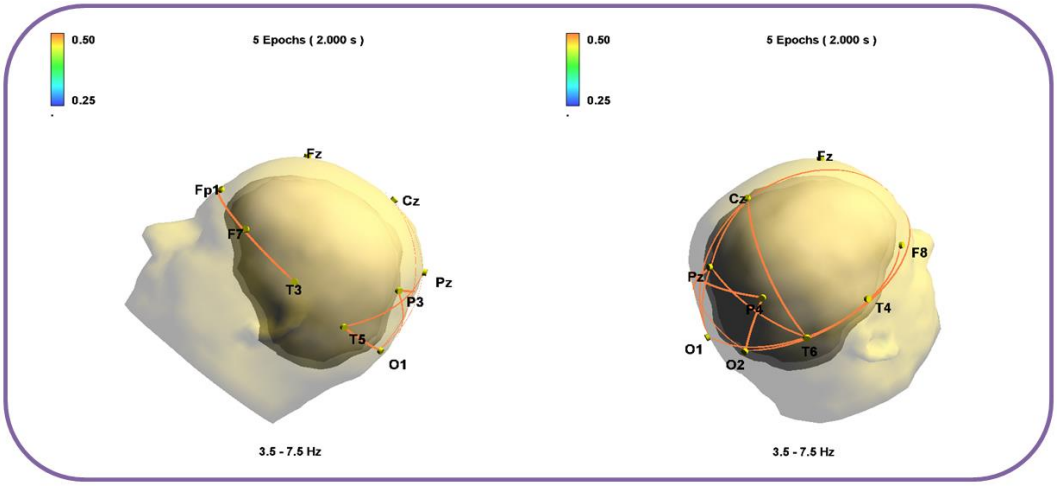


Figure no. 5 Amplitude of coherence (0.25 - 0.50 interval) for the session where the untrained subjects were inductors (5 connections with the receptors)
(Manolea, A. 2014)

[10] D.E, Amos, L.H., Koopmans „Tables of the distribution of the coefficient of coherence for stationary bivariate Gaussian processes". *Monograph SCR-483*, Sandia Corp., Albuquerque, New Mexico, 1963, p. 56.

This fact could mean that the specific training of trained subjects can generate higher efficiency in the distal psycho-informational influencing, and at the same time a higher immunity to outside influences, regardless of their nature.

Conclusions

The EEG recordings can be a useful, viable and safe instrument to highlight the distal psycho-informational influence. The extraction of the information packed in the structure of EEG recordings is a very laborious activity which at the same time requires a profound understanding of the dynamics of neural networks involved in the subliminal transfer of information. Any normal healthy subject can perform this transfer, but the most efficient ones are those with specific training. Distal Psycho-informational Influence can occur with or without intention, its mediator being the emotion manipulated in specific manner. Therefore, we can say that there is the possibility to modulate the behavior of any target subject to make it impossible for him/her to reach the established goals. The reciprocal situation is real (seems to be also more ethical) as the target subject can be supported in reaching the established goal by using his/her to a maximum.

Acknowledgement:

This work was made possible by the financial support offered by the Operational Sectoral Program for the Development of Human Resources 2007-2013, co/financed by the European Social Fund, in the project POSDRU/159/1.5/S/138822, with the title "Transnational Network of Integrated Management of Intelligent Doctoral and Post-doctoral Research in the Domains “Military Sciences”, “Security and Information” and “Public Order and National Security” - Continuous Training Program of the Elite Researchers –“ SmartSPODAS”.” A Project Co-financed from the European Social Fund by the Operational Sectoral Program for the Development of Human Resources 2007-2013 "Invest in PEOPLE”

BIBLIOGRAPHY:

1. ***, *Strategia de securitate naţională a României*, Bucureşti, 2001.
2. Brazdău, O. "Constiinta si misterele fizicii cuantice" *Buletinul psihologiei transpersonale*, Numărul 7-8/2003, http://www.arpt.ro/RO/TPBuletin/7-8-2003.htm, accesat 11.11.2012.
3. Durka, P. J., Zygierewicz, J., Klekowicz, H., Ginter, J., & Blinowska, K. J. “On the statistical significance of event-related EEG desynchronization and synchronization in the time-frequency plane”. *Biomedical Engineering, IEEE Transactions on*, 51(7), 1167-1175, 2004.
4. http://sccn.ucsd.edu/eeglab/index.html, accessed April 2014.
5. http://sccn.ucsd.edu/eeglab/index.html, accessed Aprilie 2014.
6. Manolea Aliodor “Considerations on distant psycho –informational influence in warfare”. *International Conference „STRATEGIES XXI”* „Carol I” National Defence University, Bucharest, Romania. April 18 – 19, 2013,ISSN 2285-8415, ISSN-L 2285-8318, (2013):577.

7. Manolea Aliodor “Items required to elaborate experiments on distal psycho-informational influence”. *International Conference „STRATEGIES XXI”* „Carol I” National Defence University, Bucharest, Romania. April 18 – 19, 2013-03-29, ISSN 2285-8415, ISSN-L 2285-8318, (2013):585.
8. Manolea, A. “Influenţa psihoinformaţională distală ca parte a influenţei informaţionale de intelligence”. *Academia Națională de Informaţii “Mihai Viteazul” International conference „Intelligence in the knowledge society” Bucharest, Romania, October 19th 2012. Biblioteca electronică a Academiei Naţionale de Informaţii (ANI), Colecţia "ANI - Mihai Viteazul", ISBN 978-606-532-062-3.*
9. Manolea, A. „Fundamente epistemice ale influenței psihoinformaționale distale”. *Buletinul UNAP nr.1/2013, pp. 378-382.*
10. Manolea, A. *Acţiunea beligenă şi influenţarea psihoinformaţională distală,* referat Scoala Doctorală Ştiinţe Militare şi Informaţii, UNAp, Bucureşti, 2012, pp.4-65.
11. Manolea, A. *Condiţionarea psihosomatică. Psihodiagnoză şi intervenţie psihoterapeutică folosind stările modificate de conştiinţă*, Universitatea Bucureşti, Scoala doctorală de Psihologie şi Ştiinţe ale Educaţiei, Departamentul Psihologie,Teza de doctorat, Manolea, A. “The cibernetics’subtle energy of the human being. Fundaments of the neutral theory referring to the living beings’ system”. Doctoral Thesis in Sciencies, Complementary Medicine, *The Open University for the Complementary Medicines*, Colombo, SriLanka, 2000.
12. Manolea, A., 2014, “Brain to brain connectivity during Distal Psycho-informational Influence sessions, between spatially and sensory isolated subjects”, *Romanian Journal of Experimental Applied Psihology PSIWORLD Bucureşti, Octombrie 2014*, in press.
13. Manolea, D.E, Manolea, A. *Influenţa distală - Teoria şi practica vindecării la distanţă*. Aldomar Extrasenzorial Publishing House, Bucharest, 1997.
14. Pfurtscheller, G., Lopes da Silva, F. H. , “Event-related EEG/MEG synchronization and desynchronization: basic principles”. *Clinical neurophysiology*, Vol. 110, No. (November 1999), pp. 1842-1857.

CYBER DEFENSE AND CITIZENS RIGHTS IN THE VIRTUAL ENVIRONMENT

Alexandru ION
PhD Student at the Faculty of Political Science, University of Bucharest, Romania,
ion.alexandru@fspub.unibuc.ro

Resume: *This paper will focus on threats from the Internet and how they have a direct impact on the today international relations. The online environment is available today to millions of people around the world via computer and phone. The potential of this service is unlimited, from a simple navigation to cyber terrorism. We need a better security of the Internet, but also respect the privacy of the civilians, so the following question arises: "How can we counter cyber terrorism, and at the same time respect the privacy and freedom of individuals in the online environment, given that accredited institutions have access to particular information that can be abused?" We will find the answer to this question when we identify the state / states capable of satisfying both criteria.*

Key words: *confrontation, cybernetics, vulnerabilities, cyber terrorism, conflict, internet*

Introduction

The form of conflicts in the international relations has been modified in the 21st century through technological development and also because of the more active role played by the citizens in politics. The interests may vary, as the financial support and the human resources, depending on each international political actor[1]. No wonder, that the Internet, at the beginning was a harmless mean of communication and data transfer, over these past few years has become an efficient way to serve the interests of the countries in conflict issues. The way in which the Internet has become a weapon for defensive/offensive purpose differs from case to case. Many countries have faced problems in international cyber war, most of them becoming victims in this war against states experienced in this area. Countries such as China, Russia, USA, UK, found in the Internet, a way that can increase their influence internationally and at the same time attacking their rivals by any means[2]. Since anyone has access to internet today, a cyber-attack is possible from any person and directed against: their own country, an allied country, rival country or a simple person on the internet.

The field of cyber confrontation is part of the security studies, where the topics on the subject are numerous, however in my work I chose to address two important issues: legislation on human rights and freedoms and cyber warfare in international relations. Interstate conflicts have direct consequences for each of us, and in this way recourse to infringement of privacy on the Internet, the need to access more information. I will use as a case study in this paper the USA, China and the European Union wanting to know which of these concentrate on a balance between individual rights and promoting an effective cyber defense system. I will try to use the limited literature to treat this subject in a manner as explicit and to formulate a research paper can bring a significant contribution.

[1] Athina KARATZOGIANNI, *Cyber conflict and global politics*, Routledge, New York, 2008, p. 27.
[2] Ronald DEIBERT, *Access controlled: The shaping of Power, Rights and Rule in Cyberspace*, The MIT Press, Massachusetts, 2010, p. 4.

Representation of individual rights on the Internet and reducing control methods by governments wishing to invade the privacy has become a priority for the UN, international organizations pursuing human rights, and groups like Anonymous. Based on UN initiative protection, promotion and guarantee of freedom on the Internet, I follow in my research project the impact that was produced in the international relations[3]. Assuming: an ideal defense system and avoid cyber intrusion in the private sector. Research question is: How can we combat cyber terrorism, and at the same time respect the privacy and freedom of individuals in an online environment, given that accredited institutions may be abuse of private information? The manner in which states have responded to this initiative is an interesting topic that I will cover in the first chapter, a careful analysis of the changes and benefits to government and the governed, using legislation. In the second chapter we have the focus changes between international actors, and positive and negative effects, researching what international relations theory is confirmed in diplomacy. Finally, in the conclusions I will restrict my research essential information on the area.

1. A view on rights issues

I will start this chapter with a brief overview of the UN decision on human rights and freedoms on the Internet. After years of intense discussions and negotiations the resolution 20/8 dated on 05.07.2012 was adopted without vote. It states:

"The promotion, protection and enjoyment of human rights on the Internet

The Human Rights Council,

Guided by the Charter of the United Nations,

Reaffirming the human rights and fundamental freedoms enshrined in the Universal Declaration of Human Rights and relevant international human rights treaties, including the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights,

Recalling all relevant resolutions of the Commission on Human Rights and the Human Rights Council on the right to freedom of opinion and expression, in particular Council resolution 12/16 of 2 October 2009, and also recalling General Assembly resolution 66/184 of 22 December 2011,

Noting that the exercise of human rights, in particular the right to freedom of expression, on the Internet is an issue of increasing interest and importance as the rapid pace of technological development enables individuals all over the world to use new information and communications technologies,

Taking note of the reports of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, submitted to the Human Rights Council at its seventeenth session, and to the General Assembly at its sixty-sixth session, on freedom of expression on the Internet,

1. Affirms that the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights;

2. Recognizes the global and open nature of the Internet as a driving force in accelerating progress towards development in its various forms;

[3] http://ap.ohchr.org/documents/alldocs.aspx?doc_id=20280, Resolution on human rights on internet, A/HRC/17/27, 2011, accessed on: 20.03.2015

3. Calls upon all States to promote and facilitate access to the Internet and international cooperation aimed at the development of media and information and communications facilities in all countries;

4. Encourages special procedures to take these issues into account within their existing mandates, as applicable;

5. Decides to continue its consideration of the promotion, protection and enjoyment of human rights, including the right to freedom of expression, on the Internet and in other technologies, as well as of how the Internet can be an important tool for development and for exercising human rights, in accordance with its programme of work."[4].

Due to the initiation of the UN resolution, we understand that states have the obligation to respect civil rights on the Internet, however not everywhere is the case. The best example is China, which although is a modern and competitive country like worldwide democracies, it has strong control over national Internet[5]. Censorship was imposed by the government in Beijing on the internet since the 2000; the action was recognized as the "Great Firewall of China"[6]. Among the known methods in which the Chinese government issue penalties for breaking the law on the internet include: arrest, rehabilitation, and fine, everything to maintain order[7]. Although at first glance we consider imposing censorship an affront to human rights, however government stability, reducing incitement to riot, banning adult material and a tougher control over information to citizens is an important advantage of a communist regime. This will restrict individual rights in favor for a better security. However in the past few years, China is facing an increasing number of breaches in national censorship system, this demonstrates the desire for freedom on the Internet from both within the state and outside it through young people[8].

Discussing the case of China, we observe small changes here, so we will further discuss a state located on the opposite side, the United States, where freedoms are guaranteed on the Internet[9]. However even capitalist countries like the US, proved that they are more interested in national security despite civil rights violation, giving as an example the NSA[10]. Constant surveillance of its citizens on the Internet is a violation of privacy and confidentiality[12]. Several human rights organizations have protested against the government of the White House after the incident with Edward Snowden, surpassing the country among the world's most democratic states. Conversely US interests were not limited to issues of national interest, they entered and private sphere, and here we fall initiatives: SOPA (Stop Online Piracy Act) and ACTA (Anti-Counterfeiting Trade Agreement). About these programs can add that aim to protect the interests of large US companies that have losses due to internet piracy them causing damage of thousands of dollars annually.

When we discuss individual freedoms on the internet the ideal representative is the European Union, providing a much greater freedom of citizens on the Internet, unlike the US. Worth mentioning is the Factsheet on the "Right to be forgotten 'ruling (C-131/12) European

---

[4] http://ap.ohchr.org/documents/alldocs.aspx?doc_id=20280, Resolution on human rights on internet, accessed on: 20.03.2015

[5] https://freedomhouse.org/country/china#.VIiPmXuPVoM, Freedom House accessed on: 21.03.2015

[6] Pippa NORRIS, *Public Santinel: News Media & Government reform*, The World Bank, Washingston, 2010, p. 360

[7] http://www.nytimes.com/2012/12/29/world/asia/china-toughens-restrictions-on-internet-use.html?_r=0, China toughens restrictions on internet use, accessed on: 21.03.2015

[8] http://www.huffingtonpost.com/2012/02/29/china-firewall-breach_n_1308836.html?, China firewall breach, accessed on: 21.03.2015

[9] https://freedomhouse.org/country/united-states#.VRaVH-G1doM, Freedomhouse, accessed on: 21.03.2015

[10] http://www.spiegel.de/international/topic/nsa_spying_scandal/, NSA spying scandal, accessed on: 21.03.2015

[11] http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data, NSA tools collect everything a user does on the internet, accessed la data de: 25.04.2015

Commission, 2012[12] document by which every European citizen who feels offended by online material related to his person, may request withdrawal them. But more important than that is the "EU Code of rights in the online environment" in which Section 1, Chapter 4 (1), provides: "Every individual has the right to adequate protection of their personal data.[13]"And also paragraph 2: "Individuals are entitled to receive from individuals and businesses that have some of their personal data in the obvious such as websites, databases, service providers, etc., and correct or delete such data if it is incomplete or inaccurate[14]. Therefore secret services of the Member States play an essential role in maintaining a balance between the rights of citizens and maintaining national security and protect government interests[15]. Threats are more numerous every day, therefore aims to develop a system and how best to meet the needs for national and individual.

In addition to the general vision of online rights infringements by national authorities want to raise the issue hackers pose a threat to personal information and financial ones. Only in 2014 one of the most representative virus threat was "Heartbleed" known to enter social sites such as Facebook, Instagram, Pinterest, Tumblr, Google and Yahoo[16]. The recommendation of these companies after the attack was to change our passwords. They also took the initiative to form a joint program of defense against future threats, each allocating an amount of $ 100,000 annually[17].

The result of research analyzing the above events has reached three distinct results that will fit in states where national policy towards freedom that the Internet offers: free internet, semi-free internet and censored. I wish to make an observation on the first category, free internet, not only is guaranteed by law, but it also actively promotes this idea. Talking further about the semi-open Internet, where the government intervenes and oversees its citizen's intense activity in defiance of human rights. With limited freedom and censor the Internet, defines national policy authoritarian states characterized by control of access to the Internet, where online privacy rights there. I placed at the top of the Internet free EU states, also United States we have cataloged in the second category of semi-free Internet and China belongs to the third category of Internet censorship.

2. The Cyber War

The term "cyber war" could not be provided with a concrete definition, being very controversial in the international community. The main resource of this war is the information itself and its damage by careful speculation obtained vary, handling and pushing people to revolt to millions of dollars in damages. In this chapter I want to remember the concepts of "cyber espionage" and "cyber terrorism". We define the term cyber espionage fraudulently entering into private or government information bases and their transfer without consent of the owner. The second concept relates to cyber terrorism attacks on hardware devices and software via the Internet aimed at causing irreparable damage.

---

[12] http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf, Factsheet data protection, accessed on: 21.03.2015

[13] https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Code%20EU%20online%20rights%20RO%20final.pdf, Code EU online rights, accessed on: 24.04.2015

[14] https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Code%20EU%20online%20rights%20RO%20final.pdf, Codul UE al drepturilor in mediul online, accessed on: 24.04.2015

[15] Tom DYSON, Theodore KONSTADINIDES, *Europe Defense Cooperation in EU law and IR theory*, Palgrave Macmillan, Hampshire, 2013, p. 19

[16] Office of the Privacy Commissioner of Canada, *Privacy and Cybersecurity: Emphasizing privacy protection in cyber security activities*, 2015, p. 1

[17] http://mashable.com/2014/04/24/facebook-google-microsoft-join-forces-to-prevent-another-heartbleed/, Facebook, Google, Microsoft Join Forces to Prevent Another Heartbleed, accessed on: 23.04.2015

Next we examine changes in bilateral and multilateral relations between states as a result of increased cyber warfare. Since 27 April 2007, when Russia attacked the official websites of Estonia, causing great damage to the government in Tallinn, demonstrating the existence of a new weapons NATO forces in international relations[18]. Also worth mentioning is the Russian-Georgian war, when Russia attacked Georgia all sites showing her inability cyber defense. Every country in the world their own arrangements for the preparation of a cyber defense which match the internal political environment. Among the most relevant examples of this is the UK, announcing publicly that threats via the Internet are real ones. A measure taken by the Conservative government is launching a campaign to recruit IT experts to create a team to combat the threats initiated by the Ministry of Defence[19]. Latvia is another European who noted that virtual environment security is very important, which is why he began recruiting a team to counter international threats[20]. Experts explain that unlike a real opponent, the opponent can come online from anywhere in the world, even within the state from a state allied or enemy. Austria, the first state is not a NATO member, decided to join the Alliance Center of Excellence of cybersecurity[21]. Ministry of Defence of Japan took the initiative establishment of a team of about 90 people, as the unit of cybersecurity to protect national interests in the virtual environment[22]. Under Obama, the US cyber defense budget increased over time, wanting a greater focus on combating attacks faced by the country.

Current international situation proves one thing: the trend of multipolarity, unlike the last century, where the world was divided into spheres of influence bipolar. As we can see, is approached a different perspective, but they all share one thing: fighting threats by the Government through specialized recruitment of a new kind of war. Multilateral treaties based on compromises the potential to give rise to effective cyber security projects, as I mentioned above about Alliance Center of Excellence of cybersecurity.

Financial Report of the World Economic Forum in 2014 clearly demonstrates and gives a warning on the issue of effective cyber defense system effectively bring international loss of around 3 billion by 2020[23]. Descendants of increasingly large data obtained digitally converts them into vital targets for attackers who want to interfere with governmental and international systems. From this we can deduce that the targets by aggressors since they have a weaker defense system, the more easily attacked. As James B. Comey also mentions in his speech at the International Conference on cyberdefence Forham University of New York, 2015: "Our life has changed thanks to the Internet, and everything is a threat evolved.[24]"

The consequences of inefficient state cyber defense system: closing sites, information theft, espionage, but I will focus on the most relevant. Among the many threats facing citizens and public institutions on the Internet every day, we remembered viruses and best known of these is Stuxnet, preconceived to destroy industrial systems. Its presence was confirmed both in the US, Europe and Asia, in Iran attacking a nuclear systems, causing huge

[18] http://www.theguardian.com/world/2007/may/17/topstories3.russia, Russia accused of unleashing cyberwar to disable Estonia, accessed on: 21.03.2015

[19] http://www.bbc.com/news/uk-24321717, UK creates a new cyber defense force, accessed on: 21.03.2015

[20] http://www.dw.de/latvia-launches-cyber-defence-unit-to-beef-up-online-security/a-17471936, Latvia launches cyber defense unit to beef up online security, accessed on: 21.03.2015

[21] http://www.defensenews.com/article/20140512/DEFREG01/305120014/Austria-First-non-NATO-Nation-Join-Alliance-Cyber-Defence-Centre-Excellence, Austria first non-NATO nation join Alliance cyber defense center, accessed on: 21.03.2015

[22] http://www.janes.com/article/35956/japan-establishes-cyber-defence-unit, Japan establishes cyber defense unit, accessed on: 21.03.2015

[23] World Economic Forum, *Risk and responsibility in a Hyperconnected world*, 2014

[24] http://www.fbi.gov/news/speeches/addressing-the-cyber-security-threat, International Conference on Cyber Security, Fordham University, accessed on: 23.04.2015

damage[25]. The second case is the Russian virus Rocra, who for years has stolen government information from countries that have not detected[26]. Daily notifications on threats in this area, data are available in the report of the Strategic and International Studies Center, aiming at online crime carefully[27]. We see from these examples of what is needed and priority adaptation cyber defense strategy.

Individualistic tendency of states to the problem of cyber conflict demonstrates the method of compromise between national public and private sphere to achieve the best results in terms of security. Note also the diplomacy between states, we can see that they confirm the theory of realism in international relations, where states act in order to achieve their interests. Vulnerabilities of a defense systems compromise the information in heritage and further damage resulting is huge. Threats are becoming more numerous every day, therefore the budget allocated by the states to improve cybersecurity is increasing from year to year in direct proportion to the threats they face.

Conclusions

I followed closely the effects of involvement of the individual in political life and notice the changes it brought in a short time in a field so new. We went through two chapters of research seeking answers to the question: "How can we combat cyber terrorism and at the same time respect for privacy and freedom of individuals in an online environment, given that accredited institutions may be abuse of this information?". I noticed that each state has adapted its own policy on the subject under discussion and the methods are determined by history and international experiences. While Russia prefers a more aggressive approach on cyber security, China seeks to impose censorship to control the interior and exterior threatening. The United States of America has an intrusive approach in people's lives, in order to have an efficient cybernetic system. Instead member states of the European Union took a different approach on the situation choosing a balanced way, seeking to satisfy both sides.

The United Nations plays an important role in defining the future of bilateral relations and respect for individual rights via the Internet initiative. However it is not sufficient, it is necessary involvement of powerful states and other international organizations. From studying primary bibliography consists of: treaties, legislation and interviews, we answer the question of research concluding that meets both criteria EU countries such as cyber security and rights online. If it says my research hypothesis by demonstrating the existence of an area of compromise, simple and effective. After research results in Chapter 1 we categorized states according to civil rights on the internet, the European Union entered into the first category, free internet, US Internet semi-free ranging and China as part of the third category of internet censorship . The cooperation of states and international organizations to develop the strategy limited, but it is interesting to watch now[28]. And the reason I say this is the real possibility of a war through the Internet is a threat that must be taken into account. Another perspective on this domain confers international organizations of human rights, which repeatedly criticized virtual espionage[29]. This subject can be interpreted in several ways

[25] http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11, Stuxnet was far more dangerous than previous thought, accessed on: 21.03.2015

[26] http://www.pcworld.com/article/2025328/red-october-malware-discovered-after-years-of-stealing-data-in-the-wild.html, Red October malware discovered after years of stealing data in the wild, accessed on: 21.03.2015

[27] http://csis.org/program/significant-cyber-events, Significant Cyber Events, accessed on: 23.04.2015

[28] Daniel VENTRE, *Cyber Conflict: competing national perspectives*, ISTE Ltd, London, 2012 , p. 182.

[29] Tom DYSON, Theodore KONSTADINIDES, *Europe Defence Cooperation in EU law and IR thory*, Palgrave Macmillan, Hampshire, 2013, p. 19.

depending on international political actor and interests. The realism theory is confirmed by research carried out in Chapter 2, from which we deduce the need to adapt to current changes in actions to increase security at the expense of international ideals. However, it is necessary to adapt our society given the changes that occur to counter emerging threats and we follow our interests while we enjoy the protection of the rights not abuse this freedom[30].

Cyber security represents a new world to explore for us having different possibilities that a few years ago seemed impossible to create. It is necessary to study the area discussed, as it has a direct impact on us, the way we get information, how we learn, how to communicate, etc. New methods are being developed every day by international political actors in order to obtain an advantage over competitors. The information in this case is essential, and also written articles and conferences on the subject should be a top priority.

BIBLIOGRAPHY:

1. ANDRESS, Janson, Steve WINTERFELD, *Cyber warfare: Techniques, Tactics and tools for security practitioners*, SYNGRESS, 2013
2. BAYLON Caroline, *Challenges at the Intersection of Cyber Security and Space Security: Country and International Institution Perspectives*, Chatham House, 2014
3. CAVELTY, Myriam Dunn, *Cyber-Security and threat politics: US efforts to secure the information age*, Routledge, New York, 2008
4. DEIBERT, Ronald, *Access controlled: The shaping of Power, Rights and Rule in Cyberspace*, The MIT Press, Massachusetts, 2010
5. DYSON Tom, Theodore KONSTADINIDES, *Europe Defense Cooperation in EU law and IR theory*, Palgrave Macmillan, Hampshire, 2013
6. European Commission, Factsheet on the "Right to be forgotten" ruling (c-131/12), Bruxelles, 2012
7. KARATZOGIANNI, Athina, *Cyber conflict and global politics*, Routledge, New York, 2008
8. KLIMBURG, Alexander, *Naţional Cyber Security Framework Manual*, CCDCOE, Tallinn, 2012
9. NORRIS Pippa, *Public Santinel: News Media & Government reform*, The World Bank, Washingston, 2010
10. Office of the Privacy Commissioner of Canada, *Privacy and Cybersecurity: Emphasizing privacy protection in cyber security activities*, 2015
11. SHACKELFORD, Scott J, *Managing Cyber Attacks in International Law, Business, and Relations: In search for cyber peace*, Cambridge University Press, Cambridge, 2014
12. VENTRE Daniel, Cyber Conflict: competing national perspectives, ISTE Ltd, London, 2012
13. World Economic Forum, Risk and responsibility in a Hyperconnected world, 2014
14. http://ap.ohchr.org/documents/alldocs.aspx?doc_id=20280, The promotion, protection and enjoyment of human rights on the Internet, A/HRC/17/27, 2011
15. https://freedomhouse.org/country/china#.VIiPmXuPVoM, Freedom House China

[30] Myriam Dunn CAVELTY, *Cyber-Security and threat politics: US efforts to secure the information age*, Routledge, New York, 2008, p. 27.

16. http://www.nytimes.com/2012/12/29/world/asia/china-toughens-restrictions-on-internet-use.html?_r=0, China toughens restrictions on internet use
17. http://www.huffingtonpost.com/2012/02/29/china-firewall-breach_n_1308836.html?, China firewall breach
18. https://freedomhouse.org/country/united-states#.VRaVH-G1doM, Freedomhouse SUA
19. http://www.spiegel.de/international/topic/nsa_spying_scandal/, NSA spying scandal
20. http://www.theguardian.com/world/2007/may/17/topstories3.russia, Russia accused of unleashing cyberwar to disable Estonia
21. http://www.bbc.com/news/uk-24321717, UK creates a new cyber defense force
22. http://www.dw.de/latvia-launches-cyber-defence-unit-to-beef-up-online-security/a-17471936, Latvia launches cyber defense unit to beef up online security
23. http://www.defensenews.com/article/20140512/DEFREG01/305120014/Austria-First-non-NATO-Nation-Join-Alliance-Cyber-Defence-Centre-Excellence, Austria first non-NATO nation join Alliance cyber defense center
24. http://www.janes.com/article/35956/japan-establishes-cyber-defence-unit, Japan establishes cyber defense unit
25. http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11, Stuxnet was far more dangerous than previous thought
26. http://www.fbi.gov/news/speeches/addressing-the-cyber-security-threat, International Conference on Cyber Security, Fordham University
27. http://www.pcworld.com/article/2025328/red-october-malware-discovered-after-years-of-stealing-data-in-the-wild.html, Red October malware discovered after years of stealing data in the wild
28. http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf, Factsheet data protection

ARE ROMANIAN AIR FORCES READY TO FACE FUTURE THREATS?

Cosmin Liviu COSMA
Capt Cmder, PhD student, "CAROL I" National Defense University,
e-mail: airspider@yahoo.com

Abstract: *Besides fragmentation, unpredictability, multiple asymmetries, organized crime and terrorism, recent challenges to security require a careful reassessment of the nature of the threats, the implications being multiple in how future Alliance military forces will be required to prepare and act.*

In this context, as part of the Alliance, Romania and implicitly its air forces – in order to fulfill various objectives, such as ensuring the security of Romania and of the North Atlantic area, complying with commitments taken within security organizations etc. – have to continue the modernization processes, a continuous and substantial transformation on the conceptual, the organizational-structural and infrastructure and endowment levels being absolutely necessary..

Based on these considerations, this paper aims to identify the characteristics of the context in which the air force will have to act and of the associated implications, so that, on this basis, the operational capabilities and attributes to be generated in order to allow the air force to meet the threats of today and the foreshadowed ones can be established. In order to formulate conclusions, the deductive method was used, and, in an attempt to extrapolate past experience into future experience, the inductive method was used. To establish a systemic link between explanations, conceptual frameworks and predictions, we used a combination of theoretical systems, taxonomy or axiomatic theories for the presentation of causal relationships between external factors and the military organization (the Air Force).

Keywords: *transformation, Romanian Air Force, air force, future threats, NATO*

1. Evolution of the Romanian Air Force after the end of the Cold War

The end of the Cold War and the dissolution of the Warsaw Pact in July 1991 caused profound changes in the architecture of the security environment, leading to the adoption by Romania of a security policy based on the theory of circular defense, covering and protecting the borders. The Air Force, a basic part of Romania's army, with the changing of the security paradigm, will enter into a consistent process of reforming and restructuring in order to meet the new geostrategic realities. The *doctrine of the war of all the people* that underpinned the military defense strategies until 1991 is forgotten, *"the achievement of a modern structure, fully professionalized, with a high degree of mobility, efficient, flexible, increased deployable capacity, sustainable, having the capacity to act together and be engaged in a wide range of missions, both on national territory and beyond"*[1] being established as a *general objective* of the transformation of the Romanian Army.

This objective, formulated immediately after the dissolution of the Warsaw Pact, may seem quite ambitious, considering the specific situation of the Romanian Air Force which existed before 1990. They had a staff of 32,000 people, of which more than a third were

[1] Mihail E. Ionescu, *Etapele reformei armate în perioada post-Război Rece* (1990-2008), în *Reforma Militară şi societatea în România (1878-2008)*, Editura Militară, Bucureşti, 2009, p. 325.

civilian staff, holding approximately 512 combat aircraft whose main role was to support and protect the ground and naval forces by execution of air support missions, bombing, air reconnaissance and air lift. Their structure was built around three tactical divisions, each of which comprised two regiments with three fighter-interceptor squadrons of and one of ground attack.

Their fighter aircraft were predominantly of Soviet origin (MiG-21, MiG-23), but also a significant number of IAR-93 built in Romania. Starting December 1989 the first MiG-29 Fulcrum at Air Base 57 from Mihail Kogalniceanu started arriving in the country, flight training started in March 1990 (originally 14 MiG-29A single seater and four MiG-29UB two-seater were delivered, then other two MiG-29A and 1 MiG-29C in 1992 from the Moldovan Air Force). The MiG-29 remained in the Romanian Air Force inventory until early 2003 when they were withdrawn from activity.

In addition to these steps, measures are taken regarding the implementation of the provisions of the Treaty of Paris on Conventional Armed Forces in Europe signed by the countries of the Warsaw Pact and NATO on 19 November 1990, which entered into force on 9 November 1992. The Romanian army reduced the numbers of military equipment, both in the land forces (tanks, armored vehicles, artillery) and in the military aviation (combat aircraft - from 512 to 430). They also started a process of reducing staff numbers, aiming to reach a staff of 70,000 soldiers and 10,000 civilians in the Romanian Army. There were also downsizings in the structure of forces, the General Staff (instead of the Great General Staff and the Staffs of the categories of forces) being created, division and regiment-type echelons were exchanged for corps-type and regiment structures, and the number of armies was reduced from four to three.[2] In the Air Force, in 1993 is founded *the Air Force Staff*, by unifying the *Air Force Command* and *Air Defense* Command of Territory, the new command structure bringing together *aviation, artillery, anti-aircraft missiles* and *radar air surveillance* (since 1 June 2000, will be used the current title, the *General Staff of the Air Force*). In 1995 the communist-type regimental system was changed to one based on a structure consisting of air bases, groups and squadrons.

This first stage of reforming the armed forces and hence the Romanian Air Force is characterized by a reduced pace, *"executed in an inertial doctrinal conception, focused on territorial defense"*[3]. Thus, the adaptation processes within the air forces are aligned to the general direction of *covering the territory* from a military point of view and predominant deployment towards the borders. Taking this position is justified by a series of factors with direct impact on the regional geostrategic situation in the immediate vicinity of Romania (the dissolution of the USSR, the disintegration of Yugoslavia and the war on the Dniester in 1992, NATO's indecision regarding eastward expansion, nationalist outbursts from abroad etc.).

On the level of equipping, in the early 1990s a number of decisions are taken to modernize the platforms and weapons systems under air forces inventory and carrying out procurement programs. Thus, in 1992, following a competition to select a company to modernize the MiG-21, the Israeli company Elbit is selected, which signed a contract worth 300 million USD, representing the conversion of approximately 110 MiG-21 aircraft (UM, M and MF) into 75 Lancer A air-to-ground version (of which 71 were finally delivered), 25 Lancer C air-to-air version (26 delivered finally) and 10 Lancer B two-seaters (finally 14 Lancer B delivered). The prototype MiG-21 Lancer -A flies for the first time on 22 August 1995, Lancer –B flies on 6 May 1996 and the prototype of the air-to-air version, Lancer-C flies on 6 November 1996. The program involves integration on the existent structure of the

[2] Călin Hentea, *Armata şi luptele românilor din Antichitate până la intrarea în NATO, Breviar de istorie militară*, Editura Nemira, Bucureşti, 2002, p. 257.
[3] Mihail E. Ionescu, *Etapele reformei armate în perioada post-Război Rece* (1990-2008), p. 327.

MiG-21 of a number of avionics, navigation, communications, radar and weapons systems and on the ground the integration of training/analysis mission systems etc, allowing the execution of new missions in a different manner. All newly integrated systems are to NATO standards, which will allow in the following period for the execution of a significant number of joint exercises with international partners and culminating in the execution of the first combat missions (in peacetime) after World War II by the Romanian Air Force, **Baltica 2007** (air policing mission in Lithuania, Latvia and Estonia, performed by pilots from Air Base 71 Campia Turzii).

Other modernization programs are conducted for IAR-99 and the helicopter IAR-330, with a view to the integration of advanced avionics, navigation, communications and weapons systems etc., in order to achieve a degree of compatibility (as with the MiG-21) and performances that provide the necessary interoperability to carry out joint operations with NATO partners.

On 23 October 1996 the first two C-130B Hercules aircraft enter into Air Base 90 Otopeni (the next two on February 16, 1997), and on 14 February 2007 the last Hercules C-130H (bought from the Italian Air Force in June 2004 and then sent for execution of maintenance and modernization works at Lockheed Martin Logistics Center in Greenville, South Carolina). The purchase of these aircraft allowed the Romanian Air Force to develop a strategic airlift capability, representing a significant contribution of Romania to the NATO effort in various theaters.

Another major program of acquisition and procurement of the Romanian Air Force is started in December 2007 with the signing of an agreement between the Ministry of National Defense and Italy's Alenia Aeronautica SpA for the acquisition of seven C-27J Spartan aircraft. The first aircraft are delivered starting 2010, and in January 2015 landed at Otopeni Air Base the seventh and final C-27J Spartan contracted. Through the C-27J Spartan aircraft acquisition, Romanian Air Force become possessors of next-generation platforms, designed for tactical air transport directly into the theater, in peacekeeping operations and humanitarian operations regardless of weather conditions, day and night.

Starting 2000, a series of restructuring programs are conducted with the air forces, and in 2004 Romania has only five active air bases arranged at Turzii, Borcea-Feteşti, Bucharest-Otopeni, Bacau and Boboc, plus other two reserve bases for helicopters (Mihail Kogalniceanu and Timişoara-Giarmata). The following air bases were dismantled: 91st Air Base from Caracal -Deveselu at the beginning of 2002, 93rd Air Base from Timisoara Giarmata in August 2004, 61st Air Base from Titu-Boteni in October 2004, 57th Air Base Mihail Kogalniceanu.

On the other forces of the Air Force - air surveillance and missile air defense - to join the NATO structures, in the period 1998-2003, similar processes of reform and restructuring took place. Thus, in 1998, the two air surveillance brigades (46th Air Surveillance Brigade at Ploiesti and 41st Air Surveillance Brigade at Timisoara, established in 1965, then in 1966 the second) were dismantled, to develop a new operational structure – *Air Surveillance Centre* – with the same regiment organization into battalions and radar surveillance companies. The purpose of this reorganization was aimed to *"increase the eficiency, and flexibility of the decision-making, optimize information flow of the air situation and create conditions for the integrated military and civilian airspace management"*[4]. The new created organizational structure – in order to achieve the required compatibility for the operation in the integrated airspace of the NATO – *NATINAMDS (NATO Integrated Air and Missile Defense System)* – has undergone major transformations at the level of endowment by introducing the new

[4] Aurelian Halus, *75 ani de radiolocaţie în Armata română* în *Observatorul Militar* nr.8 (1254), 26 februarie – 4 martie
2014, p. 16.

equipment consisting of modular three-dimensional radar (3D) with long-range *FPS/ 117E (T)* and those with short-range *Gap Filler*, or by deploying Operations Centre for Air Sovereignty (ASOC).

Part of the air defense system, the actual *air missiles defense* branch was involved in successive major restructuring and endowment transformation process. In 1995, 1st Brigade Antiaircraft Missiles – as part of the Territorial Air Defense Command –, by taking into subordination 4 Antiaircraft Missile battalions and a Technical Neva battalion, becomes Antiaircraft Missiles Mixed 1st Brigade, subordinated to1st Aviation and Air Defense Corps. Since 1st of september, 2001 it will be known as 1st Brigade Air Missiles, and on 1 May 2006 a Hawk Battalion is established therein, being the first unit of surface-to-air Air Force Staff equipped with combat equipment compatible with mainframe systems of NATO air missiles. The *Hawk System* is designed to ensure ground-based air defense of important objectives from attacks by airplanes, unmanned air vehicles, or from cruise missiles attack and other aerial vehicles evolving at small and medium heights.

Amid clear goals set for accession to Euro-Atlantic structures, immediately after 1990, extensive processes are started to create a new legislative framework to achieve the organizational structure and regulatory framework that meets the operating principles of the military in a democratic state, with direct influence on all categories of forces and services. Thus in order to create compatibility between the Romanian Constitution of 1991 with Article 5 of the North Atlantic Treaty, the Constitution was amended by constitutional consecration of Romania's accession to NATO and by providing a constitutional framework for future changes in the legislation on national defense.

For this, by republishing the Romanian Constitution in 2003, is created the framework for passing *Law no. 22/2004 for Romania's accession to the North Atlantic Treaty* signed on 4 April 1949. Changes also occur to *Law. 80/1995 on the status of the military, Law no. 384/2006 on the status of soldiers and non-commissioned officers (NCOs)*. For defining and fulfilling Romania's national security objectives for defense, *Law no. 473/2004 on defense planning* is passed, and, in accordance with its provisions, defense planning documents are developed: (1) *The National Defense Strategy; (2) Government Program; (3) Defense White Paper; (4) Military Strategy; (5) Directive for defense planning; and (6) Major programs and operational planning for employment of the military forces*.

In 1993 Romania formally submits its candidacy for membership in NATO, and a year later becomes the first state to respond to the invitation to participate in the Partnership for Peace (PfP), the first state in Central and Eastern Europe acceding to the PfP. For the admission of new members, NATO launched in April 1999 the MAP - Membership Action Plan, which established objectives, measures and deadlines for accession to NATO. In compliance with its provisions, Romania prepares and presents its own National Plan of preparation for accession.

On 21 November 2002 at the Summit in Prague - based on an assessment of progress of the candidate countries, the Heads of State and Government of NATO member countries decided to invite Romania to begin talks to join the North Atlantic Alliance. Along with Romania are invited to discussions Bulgaria, Estonia, Latvia, Lithuania, Slovakia and Slovenia.

The Accession Protocol was signed at Brussels on 26 March 2003 and, on 29 March 2004, Romania became a full member state of NATO, following the deposit of the instruments of ratification with the US State Department, which will be the start of a sustained process of transformation of the Romanian Army to *"broaden the range of objectives and processes to include structuring and preparation for participation in collective defense,*

improving its capacity for the full range of crisis management operations and those for multinational operations to combat terrorism."[5]

The implications of the transformation on the Romanian Air Force will be multiple - targeting the conceptual, organizational and functional levels and the infrastructure - with direct manifestations on the doctrine, force structure, instruction and operations, technologies and arms respectively.

2. Aspects and theories of the Romanian Air Force transformation in the new security paradigm

Since the end of the Cold War, mainly since Romania was accepted as a member of the North Atlantic Alliance, the air forces - along with the other military categories - have undergone substantial processes of transformation in order to change them into modern force structure, small, highly specialized, properly equipped, highly deployable in the theater, interoperable and sustainable with multidimensional protection, integrating a flexible command and control structure[6], to enable them to fulfill their responsibilities regarding national defense, and also to be able to give joint and multinational response within the Alliance to current and future threats specific to an extremely complex security environment, *"whose evolution is difficult to estimate and managed due to huge volume of data and the high degree of unpredictability"*[7].

The correlation of the Romanian Army's transformation with the transformation process of the Alliance provided the medium of the manifestation of this transformation as a result of reconsidering ways of response by NATO, from those specific to rigid organization in a purely defensive posture, to those of the current organization, involved in military operations conducted outside the traditional area of responsibility, wherever the interests of the Alliance requested. In this context, the new strategic guidelines and transformation of NATO direct the transformation process of Romania's future force structures, aiming to generate those military capabilities that allow them to act against both conventional and asymmetric threats, by executing the entire range of missions, from crisis prevention to humanitarian operations and high intensity war.

Transformation at the level of concepts involves developing and testing new approaches on how to conduct the war, capabilities and operational concepts or organizational constructions through simulations and exercises conducted in a manner designed based on emerging challenges and opportunities. The results of this evaluation by simulation are destined to refining and adjusting new concepts, so that after this, by using powerful mechanisms for implementation, they can be implemented in developing the *transformational military capabilities*.[8]

Thus, a number of theories were developed - based on internal factors of the military organization, contextual factors of the security environment, and the role of integrating new technologies - designed to provide the necessary framework for the development of appropriate military capabilities and relevant to the current and future security context. Generating capabilities is a process built around distinct functions, which are interdependent, along with *concepts* being also *the human factor, the assets/infrastructure and instruction*[9].

---

[5] Ministerul Apărării Naţionale, *Strategia de transformare a Armatei României*, Bucureşti, 2007, p. 3.
[6] *Ibidem.*
[7] Mihail Orzeaţă, *Războiul Continuu*, Editura Militară, Bucureşti, 2011, p. 25.
[8] US DoD, Office of the Secretary of Defense, *Military Transformation – A Strategic Approach*, Director, Force Transformation, Pentagon, Washington, US p. 3.
[9] Christopher Ankersen, *Capabilities and Capacities* în *Transforming National Defense Administration,* School of Policy Studies, Queen's University Kingston, Ontario, Canada, 2005, p. 13.

The importance of the transformation at the conceptual level lies in the crucial role involved in generating operational capabilities, updating current concepts, and the development of new concepts being required in terms of *combat functions*, understood as a fusion of the human factor, platforms, weapons and munitions systems, infrastructure, ideas, skills and equipment.

According to the theories of the US Department of Defense regarding the military transformation process, developing innovative concepts - which meet the requirements of transformation strategies - is the most important facilitator to build *transformational military capabilities* (involving technology, processes, organization and the human factor[10]).

From the perspective of conceptual transformation of the Romanian Air Force, in order to provide the necessary framework guidelines for planning and conducting air operations, in 2000 the *Air Force doctrine* is developed and then revised in 2005 and renamed the *Air Force Doctrine for Operations (DOFA).* Intended to determine the set of principles guiding the use of air forces in all types of operations executed for meeting their goals in peacetime, in crisis and in war, the DOFA is a document that is based on the study of national doctrines of a higher order and of NATO doctrines, and of some NATO countries, as well as the analysis of experiences in conducting national and multinational exercises and military actions of the air forces of the states which participated in various conflicts in recent decades.

As a result of diversification and amplification of asymmetric risks, of the manifestation of instability and crisis phenomena, and the maintenance of traditional hotspots of tension and of the expression trends for geopolitical redesigning of certain areas (Central Asia, Caucasian-Caspian area, the Extended Middle East, Africa etc. [11]) - amid the growing role of the international community and of certain organizations specialized in solving and crisis management - within NATO are implemented processes to *"increase the capacity to intervene in crisis situations and increase the possibilities of projecting the forces into spaces of interest, while continuing the transformation of mechanisms, structures and decision-making procedures"*[12].

The adoption of this *comprehensive approach* by NATO led to the conceptual alignment of the Romanian Army to build the necessary framework for the development of a force structure able to participate in the full range of missions, from crisis prevention to humanitarian operations and conflicts of high intensity. In this context, the 2007 *Strategy for Romania's Armed Forces Transformation* was developed, representing the enhanced vision on future military force structures and operational capabilities necessary to fulfill the joint and international missions within NATO or other alliances with the partners. Basically, it is the moment when in the military lexicon of the Romanian Army appears the concept of *military transformation*, associated to the phenomena of reforming, restructuring, innovation, modernization etc, with all the terminology-related and procedural implications, leading to a better permeability of the conceptual framework of the Alliance (of which were developed and evolved the framework for Romania and other Member States), and facilitating the transfer of ideas, precepts, etc.

The Romanian Armed Forces Transformation Strategy, in the context of the level of ambition, stresses the importance of the capacities that the Romanian air force generates to accomplish the tasks and roles for the defense of the Romanian territory on the one hand, and to meet commitments to NATO, EU other regional organizations on the other hand, also outlining attributes of future aerial force structures, which will be *"modern, fully professionalized, with a high degree of mobility, efficient, flexible, sustainable, fit for fighting, tailored to the mission, deployable at long distances or on global scale, which can quickly*

---

[10] *Ibidem.*

[11] MApN, *Strategia de transformare a Armatei Românei*, p. 3.

[12] *Ibidem.*

respond to crisis and participate in joint and/or multinational operations"[13]. The conceptual framework provided by DOFA is also completed by introducing, even if briefly, a number of emerging concepts (Effects based operations/capabilities and Network centric operations) and concepts related to military capabilities development that will allow air operations outside the traditional area of responsibility of the Alliance, in an expeditionary manner.

The processes associated with *air forces transformation at organizational* and *structural level* must be analyzed both in the broader context of military organization, as part of it, but also in a particular one, specific to the aerial instrument, characterized by distinct attributes of differentiation from other categories of weapons, services etc. The military organization is characterized on the one hand by its own internal customs and repetitiveness, considered inertial in relation to the action of transformation processes, but also by unique features on the other hand, as high specialization, stability, authority and well defined hierarchy, oriented towards fulfilling objectives and tasks assigned.

Some theories consider the military body to be *"a large bureaucracy, designed to produce routine and orderly action, preferring continuity and not change"*[14]. To maintain its relevance, it is forced to reevaluate and reconfigure the organic structures based on analyzes of factors and sources that require organizational and structural change (policy and strategy, organizational and cultural norms, new technologies, etc.). Such an analysis centered on objectives and strategy should provide information about the performance of the military organization - with direct applicability also in the case of the air forces - by identifying answers to the following set of questions on the basic principles of the organizational structure: (1) Are the structure and architecture of the organization able organization to meet its goals and strategies? (2) Do the organization's structure and architecture represent a means to support or enable the change of internal culture? (3) Is the structure so designed as to create the flexibility necessary to the processes by which resources can be transferred and used in accordance with the new priorities? (4) Is the structure so designed as to be supported financially?

In order to achieve combat capability, a high degree of interoperability and capabilities radically transformed, foreshadowed in the Romanian Armed Forces Transformation Strategy, the design processes of the future air forces of Romania will have to be centered around a set of requirements and principles consisting of: (1) *effectiveness and efficiency; (2) standardization of internal processes within the organization; (3) cooperation / interoperability; (4) sharing information and providing feedback; (5) opportunities on career advancement; (6) the composition of the governing bodies; (7) the legal-normative aspect; (8) professional satisfaction and motivation; (9) continuous assessment and reassessment of the relevance of the organization.*

It is therefore crucial to understand the factors affecting the design of structures within the military organization that meets precise roles and functions, adjusted to provide the desired results in the theater. In this process of structural building, at the organizational level, it is also necessary to consider the relationship between **structure and strategy**, **structure** *and size, structure and technology*, but also the ones underlying the interaction between *structure and a highly complex and dynamic security environment*. Other issues to be considered are related to the functional relational aspect that must be met (functions, tasks, personnel organizational forms and of expression / transfer of authority - command lines, communications and procedures, etc.).

Although these principles are rooted within traditional management and classical organizational theory, they are found in a clearly outlined form, also characterizing some of the concepts of military transformation (*Revolution in military affairs*). By applying them in

[13] *Ibidem,* p. 28.
[14] Stephen Peter Posen, *Winning the Next War: Innovation*, Ithaca: Cornell University Press, US, 1991, p. 2.

organizational and structural modeling processes of the future air forces of Romania, should result in *"forces for the XXI century, smaller in size, much more specialized functionally, designed for both territorial defense and against threats specific to small scale conflicts (SSC)"* [15], defined by distinct characteristics: (1) *flexibility in doctrinal field*; (2) *strategic mobility*; (3) *configurability and modularity*; (4) *the ability to act jointly and combined*; and (5) *the versatility to operate in a conflict and military operations other than war (MOOTW).* [16]

The same *Romanian Armed Forces Transformation Strategy* (in 2007), also stresses, both in terms of *organizational-structural and functional-actional perspective* the need for the metamorphosis of the Romanian Air Force from a static structure into a powerful force, with expeditionary potential and high readiness, capable to act in a jointly manner to be able to meet the future challenges of the security environment. The above principles find applicability in the processes of designing packages that operate integrated within expeditionary groups of forces.

In the last two decades, the NATO member states' air forces have been deployed in various construction packages, configured jointly with land or naval forces, or with other air forces in a multinational manner in order to execute missions in different theaters, such as Bosnia, Iraq, Afghanistan, Libya, etc., resulting from this experience a number of lessons learned already theorized in principles and models that conceptualize the design and the ways in which the air forces will be deployed in theaters at long distances beyond the traditional areas of responsibility.

In the development of future air forces, the use of theories, such as the theory of modularity, should provide the necessary conceptual framework for the deployable structures development of the displacement capacity through the operation of the processes of formation/assembly of the air component in order to integrate it within operational groups of expeditionary forces (as temporary forms of organization). The resulting constructs will be structures based on precise functions, support squadrons consisting of functional elements, as well as air traffic control, maintenance, repair, logistics etc, for supporting combat squadrons to fulfill the operational role.

According to the same theory of organization modularity or the one of military systems, since most force structures are characterized to some extent by the ability to group, to connect through their capacity (internal mechanisms) held by categories of forces, almost all existing elements of the forces are to a certain degree modular. Some of the military organizational systems are very modular, *"they can be decomposed into a number of elements that can be mixed and matched/recombined in a variety of operational groups (temporary) without loss of functionality"*[17].

It is also the case of the air forces, being the beneficiaries of native attributes in this direction, which have an architecture composed of units that can be separated, connected and combined in various configurations, while maintaining their basic functions, continuing to interact, *"to allow exchange of resources (material or as information), by adhering to common operating procedures, or by other common technologies of coordination"*[18]. The air forces will become more modular by increasing the compatibility and standardization of organic elements, thereby increasing the number of possible configurations.

---

[15] Kevin D.Stringer, *Military Organizations for Homeland Defense and Smaller-scale Contingencies: A Comparative Approach*, Library of Congress, Praeger Security International, US, 2006, p. 3.

[16] Thomas Barnett, *Blueprint for Action: A Future Worth Creating*, 2005 în Ivan Dinev Ivanov, *Transforming NATO – New Allies, Missions and Capabilities"*, Ed. Lexington Books, Plymouth, UK, 2011, p. 47.

[17] Melissa A.Schilling şi Christopher Paparone, *Modularity: An Application of General Systems Theory to Military force Development* in *Defense Acquisition Review Journal*, US, 2005, p. 284.

[18] *Ibidem.*

3. Conclusions and recommendations

Changes in the new security environment - created by events that took place after the Cold War - led to changes of strategies in military organizations by identifying new challenges and threats, different from the above, which involved the shaping of new objectives. For members of the Alliance, this change in strategy required reconfiguration of structures and realignment of roles and functions to the new objectives, thus imposing the implementation of complex processes of transformation of the weapons categories of the military institution.

After accession to NATO and acceptance as a full member, Romania - along with most European countries members of the Alliance - followed the path of military transformation processes, using the conceptual framework developed and offered by NATO. Thus, since 2005, with the initiation of the NATO integration process of the Romanian Army, carried out under the *Accession and integration Plan of the Joint Force Commander for Bulgaria***,** *Romania and Slovenia (2004),* several measures are initiated to make operational, to equip forces and to develop military capabilities undertaken within the Alliance. Until 2014 are certified and affirmed 80 structures of the Romanian Army (part of which is represented by the air forces), part of the package of forces provided by *NATO Force Goals FG 2008*. [19]

The Romanian Air Force transformation must be understood in terms of generation of military transformational capabilities, involving issues of technological, procedural, organizational, and issues related to the human factor. At the base of these there are innovative concepts, developed both based on the experience accumulated as a result of NATO's participation in various operations and conflicts over the past two decades, and also based on theories and the results of the research and development programs pertaining to the information age.

Thus, to obtain those operational capabilities that allow generating the desired effects needed to combat tomorrow's opponents, are required significant changes at the organizational level, structure of forces, platforms, equipment and mission - *"which should be continually evolving to respond positively to requests and to exploit all the opportunities arising; in what the change is concerned... it is necessary that decisions be taken regarding which of the operational capability should be maintained or retained or changed, which ones need good development, and which one of the old ones must be removed"*[20].

Viewed in terms of adaptability, at organizational level, the air forces must have the architecture to allow reconfiguration of capabilities held in a sufficient number of alternatives to perform specific tasks in joint and multinational environments. The modularity of the new force structure is considered an indispensible attribute in the new security context, facilitating the *"mixing and adjusting of units in integrated structures in groups of expeditionary forces."*[21]

In the *functional-action field*, the new missions and roles foreshadowed will still require ownership by NATO air forces of capabilities that - *in a spatial perspective* – should allow first force design and then access to areas hard to reach, with limited infrastructure or without its existence, locations far and very far from the basic location, and - *from a temporal perspective* - the high readiness (in case stopping the genocide, similar to that present in Syria and northern Iraq where the Islamic State (ISIS) terrorist group commit unspeakable atrocities) and the sustainability of operations for long periods of time.

---

[19] Ministerul Apărării Naţionale, *România-NATO, Primii zece ani*, Bucureşti, 2014, p. 4.
[20] Kevin D.Stringer, *Military Organizations for Homeland Defense*, p. 4.
[21] Erik J.de Waard, Eric-Hans Kramer, *Tailored task forces: Temporary organizations and modularity*, Netherlands Defense Academy, Department of Management, 20 May 2008, p. 1.

The implications of using air forces in MOOTW, in future operations conducted in support of the United Nations, are less of a structural nature, imposing changes of an organizational nature. So even if involved in specific activities in support of UN missions - from providing specialized structures of command and control, communications and computers (C4), intelligence, surveillance and reconnaissance (ISR), up to the execution of search and rescue missions - *"do not require radical changes in the structure of forces, but require changes in: (1) attitudinal and reporting to this type of mission; (2) training and instruction; and (3) doctrine and planning procedures"*[22]

To manage these challenges by offering solutions to the level of involvement of forces, high-level concepts, on new missions (non-Article V) as *peace keeping and peace enforcement, peace building and maintaining peace*, were translated and aligned with the concepts of the strategic and operational concepts. This approach allows the military organization to manage a large number of roles and missions in a very complex and violent spectrum, *"while at the same time offering - by transferring in the conceptual practice area within the organization - a clear direction on how the organization see themselves, reconsiders and integrates capabilities in the force structure to generate heterogeneous value"*[23].

Romanian Air Force transformation must address all three components of air power (moral, conceptual and physical), aiming at aligning such doctrines, strategies, principles, to the standards and operational procedures of their own with those of the Alliance, but also starting and / or purchasing and procurement pursuit forces with new technologies for achieving interoperability with NATO allies. The development of air forces operational capabilities to respond effectively to current challenges and future security environment, refer to the following areas: *(1) information; (2) air surveillance, target acquisition and engagement; (3) ground surveillance; (4) attack capabilities with high-precision weapons and suppress the enemy air defense; (5) strategic airlift and air refueling; and (6) command, control and communications systems to be deployable.*

The importance of these areas is supported by attention to modernization programs, purchasing and procurement, focusing on technologies that will produce and develop the operational capacities concerned. The development of these new capabilities will contribute both to strengthen the response capacity of the entire spectrum of Alliance missions - from specific collective security or territorial defense to the stability - and to strengthen the credibility of Romania's air power in NATO.

Since 2016 – and expected by 2025 –, by entering the final stage of the transformation process (as provided by the *Romanian Armed Forces Transformation Strategy***),** long-term objectives will be achieved aimed at: *"(1) further modernization of the endowment with new equipment and achieve full interoperability with the armies of NATO and the European Union; (2) concentrating efforts and financial and human resources in order to achieve the objectives set out in the Goals and capabilities and fulfilling responsibilities within NATO and the European Union; and (3) concentrating systemic assessment of the activities focusing on the structural process of equipping and modernization of technique and equipment".*[24]

For the Romanian Air Force, both the implications and challenges are major, achieving these goals is possible only if a corresponding budget will allow further transformation processes in the conceptual, organizational, functional and the infrastructure levels. From this perspective, it is necessary both to improve the regulatory framework by

---

[22] Steven Metz, *The Air Force Role in United Nations Peacekeeping*, http://www.airpower.maxwell.af.mil/airchronicles/apj/apj93/win93/metzzz.htm, pagină accesată la 07.05.2014.

[23] Joseph Soeters Paul C. van Fenema, *Military Organizations's Capabilities for Heterogeneous Value Creation* în *Managing Military Organizations. Theory and Practice*, Routledge, US, 2010, p. 494.

[24] MApN, *Strategia de transformare a Armatei României*, p. 7.

updating or developing new concepts and doctrines and to create a completely different context of expression of processes within the organization, *"by changing the mentality, attitudes and understanding/ reporting into value, education, etc., which should facilitate the transition from reactive to the proactive expression"*[25] (finally targeting the transformational models).

Thus the extent to which Romania's air forces are ready to respond to future threats is that they will succeed in developing operational capability resulting from understanding and implementation of latest concepts developed within the Alliance (including also those relating to Effects-based Operations or Network Centric Operations), supported by acquisition and procurement processes with modern technology, the end result being both generating expeditionary structures, flexible and at a high level of training, deployable in a very short nottice, capable to act in a joint and combined manner in the full spectrum of missions and obtaining a robust national air defense system and an integrated air defense in NATINAMDS, involving the entire inventory of capabilities in a synergistic manner.

BIBLIOGRAPHY:

1. Ankersen, Christopher, *Capabilities and Capacities* în *Transforming National Defense Administration,* School of Policy Studies, Queen's University Kingston, Ontario, Canada, 2005
2. Barnett, Thomas, *"Blueprint for Action: A Future Worth Creating"*, 2005 în Ivan Dinev Ivanov, *"Transforming NATO – New Allies, Missions and Capabilities"*, Ed. Lexington Books, Plymouth, UK, 2011
3. Halus, Adrian, *75 ani de radiolocaţie în Armata română* în *Observatorul militar nr.8* din 26 februarie-4 martie 2014
4. Hentea, Călin, *Armata şi luptele românilor din Antichitate până la intrarea în NATO, Breviar de istorie militară*, Editura Nemira, Bucureşti, 2002
5. Ionescu, Mihail E., *Etapele reformei armate în perioada post-Război Rece* (1990-2008), în *Reforma Militară şi societatea în România (1878-2008)*, Editura Militară, Bucureşti, 2009
6. Metz, Steven, *The Air Force Role in United Nations Peacekeeping*, http://www.airpower. maxwell. af.mil/ airchronicles/apj/apj93/win93/metzzz.htm.
7. Ministerul Apărării Naţionale, *România – NATO, Primii zece ani*, 2014
8. Ministerul Apărării Naţionale, *Strategia de transformare a Armatei României*, Bucureşti, 2007
9. Orzeaţă, Mihail, *Războiul Continuu*, Editura Militară, Bucureşti, 2011
10. Orzeaţă, Mihail, *Globalization, Crises and World Security*, LAP LAMBERT, Academic Publishing, Germany, 2013
11. Posen, Stephen Peter, *Winning the Next War: Innovation*, Ithaca: Cornell University Press, US, 1991
12. Schilling, Melissa A. şi Paparone, Christopher , *Modularity: An Application of General Systems Theory to Military force Development*, în *Defense Acquisition Review Journal*, US, 2005

[25] Mihail Orzeaţă, *Globalization, Crises and World Security*, LAP LAMBERT, Academic Publishing, Germany, 2013, p. 126.

13. Soeters, Joseph şi van Fenema, Paul C., *Military Organizations's Capabilities for Heterogeneous Value Creation* în *Managing Military Organizations. Theory and Practice*, Routledge, US, 2010
14. Stringer, Kevin D, *Military Organizations for Homeland Defense and Smaller-scale Contingencies: A Comparative Approach*, Library of Congress, Praeger Security International, US, 2006
15. US DoD, Office of the Secretary of Defense, *Military Transformation – A Strategic Approach*, Director, Force Transformation, Pentagon, Washington, US
16. Waard, Erik J.de şi Kramer, Eric-Hans, *Tailored task forces: Temporary organizations and modularity*, Netherlands Defense Academy, Department of Management, 20 May 2008
17. www.nato.int

OPERATIONAL REQUIREMENTS IMPOSED ON THE AIRCRAFT AND INFRASTRUCTURE OF THE FUTURE ROMANIAN AIR FORCES

Cosmin Liviu COSMA
Capt Cmder, PhD student, "CAROL I" National Defense University,
e-mail: airspider@yahoo.com

Abstract: *The Air Force, by its unique attributes - speed, firepower, flexibility, power of projection of its capability on a global scale, information dominance etc. - will continue to represent the essential element in solving military conflicts at any level, regardless of the constructions and forms of involvement proposed by military and political decision makers. Effective use of the air force is however subject to a number of factors, some of which are represented by the characteristics of the aircraft and the weapon systems, as well as of the infrastructure of the air bases.*

The main purpose of this paper is - on the basis of a qualitative analysis, using the deductive method, axiomatic theories and taxonomies – to establish the attributes that the Romanian Air Force planes and infrastructure must possess to be able to respond to future challenges and threats to Romania and NATO's security. To achieve this goal, initially were identified the causal relations between tasks / roles and requirements / attributes of aerial platforms and of the infrastructure.

Keywords: *Romanian air force, fighter aircraft, infrastructure, purchasing, procurement, interoperability, NATO.*

1. Aspects of Romanian Air Force infrastructure endowment and the new context created after the Cold War

The new situation created after the Cold War - characterized by the occurrence in the close proximity to Romania of separatist, interethnic, religious conflicts, illegal trafficking of weapons, drugs, persons or other forms of cross-border crime[1], and more recently the conflict generated by the annexation of Crimea by Russia - have resulted, from a military perspective, in defining a number of national security objectives to ensure the defense capabilities needed both to guarantee national interests and to comply with obligations as a member of NATO and the European Union[2].

In this context, in order to adapt the military capabilities to the demands of the new security environment created soon after 1990, the air forces, along with other forces of the Romanian Armed Forces have undergone reforms in force structures, doctrines, concepts, preparation, equipment, and infrastructure, a process that took on substance and a uniform and consistent approach especially after Romania's accession to NATO structures in 2004.

In terms of procurement processes and those associated with the infrastructure, the procurement programs developed after 1990 aimed at: (1) *withdrawal of obsolete equipment*, which supplied the Cold War, and its replacement with modern systems that allow network operation; (2) *modernization of existing aircraft* for both combative performance increase and to obtain technical compatibility with allied platforms within the Alliance; (3) *The acquisition of aerial platforms* designed to carry troops and equipment in theaters or in support of

[1] Ministerul Apărării Naţionale, *Carta Albă a Apărării*, Bucureşti, 2011, p. 7.
[2] *Ibidem.*

peacekeeping missions; (4) *development of an integrated air traffic control system*; and (5) *development of an identify friend and foe system (*IFF*)*, NATO-compatible.

These programs were: (1) modernization of aircraft MiG-21, IAR-99 and IAR-330 PUMA helicopters, with integrated modern avionics, navigation, weapons, radar and communications systems. In addition to increased performance of discovery and fight against air and ground threats, was also obtained a high degree of interoperability with NATO allies' platforms and systems; (2) upgrading the surveillance system by acquiring the three-dimensional radar AN/FPS-117, intended both to ensure real-time data about each target in the volume of air which is sought (detection, tracking and identification of air assets that evolve at distances up to 450 km) and to control the airspace, directing our own aircraft to interception. Introducing this system allowed obtaining the technical and operational compatibility at NATO standards, by providing aerial surveillance and connecting with the NATO integrated air defense system; (3) acquisition of the remotely piloted air system (UAV) SHADOW 600, which allowed increasing the capacity to collect and share information in real time in the theater of battle, and the integration of such systems compatible with the allied systems with the control, command and information structures (C2I); (4) upgrading and ensuring assistance with landing for aircraft to NATO standards by *acquiring the Technical Land Assistance System for Air Navigation* for four airfields and heliports of the Romanian Air Force; (5) The initiation and development of the *Air Sovereignty Operational Center* (ASOC) to obtain centralized leadership capacity of actions to ensure air sovereignty, by integrating data provided nationwide both by military radars and the civilian ones; and (6) development of an *identify friend-foe system* (IFF) *DIALOG* compatible with similar NATO systems, for identifying all combat platforms evolving within the airspace of Romania.

To achieve the overall objectives of the Ministry of Defense, based on priorities defined under the *National Strategy of Defense*, the defense policy guidelines established by the *Government Program* and in accordance with the *Strategic Concept of NATO* and *NATO Ministerial Directive* – it is required that reforms continue in defense resources, and that the legal framework be modified to fit the new institutional realities, the national and international security environment and experience accumulated in theaters of operations.[3] By streamlining the processes, and by ensuring consistency of all disciplines of defense planning and coordinating them in a unitary manner (in accordance with the *Outline Model for a NATO Defence Planning Process*, presented in the Summit of Strasbourg-Kehl, on 3-4 April 2009), they tracked the development of operational capabilities of medium and long term protection. To do this, it is provided that the planning and programming of resources be made on the basis of major programs.

According to Law no. 473/2004 on defense planning, these major programs are *"all the concrete actions and measures undertaken for the creation, modernization, equipping, training, maintenance of peace and preparing for crises and war of the military units, ensuring optimal living conditions for the personnel, providing logistical support and reserve for mobilization and war, creation and maintenance of the infrastructure for military actions within the mutual defense of NATO, participation in international cooperation projects with other countries and annual resources to achieve them."* [4]

Within the Air Forces, capabilities have been developed, which, through the benefits from the strategic and operational level, have also become popular within NATO: (1) strategic airlift capabilities (participation in the *Strategic Airlift Capacity*) and tactical; (2) helicopters: SOCAT for transport (NATO and for medical evacuation - MEDEVAC), naval, and from 2010 helicopters for combat search and rescue (CSAR); (3) aerial surveillance, by

[3] Ministerul Apărării Naţionale, *Planul Strategic al Ministerului Apărării Naţionale 2010-2013*, Bucureşti, 2010, p. 8.
[4] *Ibidem.*

participating in NATINAMDS (NATO Integrated Air and Missile Defense System); and (4) the modernization of military airfields at NATO standard with radio navigation systems, landing lights and control.

Other modernization programs, equipment and infrastructure renewal were *"materialized in support of deployed forces in theaters, in the movement and transport fields, in the field of support of the host nation and in the NATO program of investment in security infrastructure (*NSIP*)"* [5].

Regarding the NATO Security Investment Programme (NSIP), developed after Romania's accession to NATO, currently a total of 50 projects are under course, which are part of 10 packets of operational capabilities, with a total financial value of 128.029 million Euro, of which NATO NSIP funds amounting to 104.106 million Euro (about 81%).[6]

Romanian Air Forces are the beneficiaries of a considerable proportion of the number of projects included in the 10 operational capability packages containing NSIP projects, in that they concern mainly operational facilities, particularly in the field of aerodrome infrastructure, insurance and maintenance of capabilities included in the NATO Integrated Air Defense and Missile System (NATINAMDS) and the improvement of network communications, of major interest in NATO.

With the outbreak of the crisis in Ukraine in 2014, a change of priorities occurs for NATO, which determines, within the Ministry of Defence, placing emphasis on increasing the operational capacity, which is reflected also in the decisions taken in the field of acquisitions/ endowment. They focused on the following priorities: the strategic program of *Multi-role Aircraft of the Air Force*, the flight program for *short-medium courier C-27 SPARTAN*, *surface to air missile system on short range HAWK*, the *IAR 330 PUMA NAVAL helicopter* programme, the program of armored transporter 8x8 PIRANHA. [7]

In the next period, to achieve a structure of forces highly sustainable and interoperable, flexible, mobile, deployable in theaters, able to participate in the full range of NATO and EU missions, as well as coalition-type missions - as reflected in the *Strategic Plan of the Ministry of Defence* - will continue the procurement in conjunction with the resources made available, the weapon systems that incorporate modern technologies, adequate, to meet the requirements of all categories of military forces and to ensure interoperability with NATO forces.

2. Requirements of bases and infrastructure elements of the Air Force Romanian in the context of future threats

The analysis of Air Forces infrastructure is required to be done in terms of roles and missions that the force structure must meet, approach justified by the type of supervenience relationship between assets - processes or infrastructure - roles/ missions. This asymmetric relationship of dependence between the two categories of properties - physical (infrastructure, bases) and procedural (roles, missions) - involves transferring the effects of the first category to the second, as a result of changes or transformations performed.

It was necessary first to define the concepts related infrastructure, air bases, respectively logistics system, processes and associated programs. Thus, NATO sense, infrastructure is *"static buildings and permanent installations required to support military forces"*[8] or "the *static items of capital expenditure which are required to provide the material support for operational plans necessary to enable the higher command to function and*

[5] Ministerul Apărării Naţionale, *România-NATO. Primii zece ani*, Bucureşti, 2014, p. 5.
[6] *Ibidem.*
[7] Mircea Duşa, *Bilanţul MApN pe 2014,* Ministerul Apărării Naţionale, Bucureşti, 10 martie 2015, TVRNEWS.
[8] NATO Infrastructure Commitee, *50 Years of Infrastructure – NATO Security Investment Programme is the Sharing of Roles, Risks, Responsibilities, Costs and Benefits,* 15 may 2001, p. 18.

various forces to operate with efficiency."[9] According to the US doctrinal documents, infrastructure is *"the provision of services, processes, facilities, and related support required for developing, generating, sustaining, maintaining, and recovering aerospace power. Infrastructure is a collection of physical elements, such as squadron operations buildings, and processes, such as the military personnel flight operations"*.[10]

Infrastructure ultimately support operations throughout the spectrum of conflict, both in garrison and in the expeditionary environment, including: (1) Installations; (2) Logistics; (3) Personnel services; (4) Health services support; (5) Headquarters and headquarters support functions; (6) Science and technology programs; (7) Test, evaluation, and target facilities and ranges; (8) Electromagnetic frequencies; (9) Non-unit training; (10) Acquisition, contracting, and financial services support; (11) Command, control, communications, computers and intelligence (C4I) systems; (12) Installation support functions; (13) Community support functions; (14) Depot maintenance; and (15Associated aerospace support systems.[11]

Airbases are locations from which operations are generated and supported, being defined as containing *facilities* and *infrastructure*. Infrastructure, as outlined above, refers to all fixed and expeditionary installations, fabrications, facilities and processes that support and control military forces. A facility means a real entity, consisting of one or more buildings, structures (including regular and temporary structures - tents etc.), system utilities, pavements, underlying lands, etc. Core functions include providing power, fuels, ammunition, water, civil engineers, services, medical, and command and control.

Beyond the services of air bases, they can be categorized on the core functions and the intensity with which they are deployed/ generated air operations. Are identified as follows: (a) *Main Operations Bases* - characterized by a developed infrastructure and support services that can meet all processes designed to support/ generate air operations throughout the full spectrum; (b) *Collocated Operations Bases* - they are usually owned and operated by an Allied force; infrastructure, the readiness and support facilities can be presented in different degrees of availability, and usually used by Air Force Reserve structures; and (c) *Forward Operations Bases* - their infrastructure can vary from one developed to one austere, usually consisting of bases that support aircraft on routes to/ from theater, bases being disposed at the closest and optimum point to theaters, performing arming and refueling activities.

Conflicts experience of the Cold War developed till present days - the most recent being the *Operation Unified Protector* resulting from the 2011 Libya - outlined Air Force air bases and infrastructure of NATO member states necessary traits to be able to carry out missions the entire spectrum of conflict in joint and multinational environment.

Missions that the armed forces of Romania will have to meet the new security context encompasses a broad spectrum, from defending national territory and to those for participation in multinational commitments undertaken under the aegis of NATO and EU organizations such as the UN and OSCE or the coalition of the willing.[12]

The characteristics of air bases and infrastructure owned by Romanian air force must be understood in terms of generation and support of air operations separate (for national defense and collective NATO), along with allies, both in the area of responsibility and outside its within expeditionary operations. Another aspect to be taken into account – expeditionary operations associated – in terms of the characteristics/ infrastructure conditions relates to Host Nation Support (HNS).

---

[9] *Ibidem.*
[10] US Air Force, *Air Force Doctrine Document 2-4.4 – Bases, Infrastrastructure and Facilities ,* 13 November 1999, p. 7.
[11] *Ibidem.*
[12] Ministerul Apărării Naţionale, *Carta Albă a Apărării*, Bucureşti, 2011, p.9.

Future air bases and their infrastructure – for supporting control and command and force structures of the Romanian Air Force, or those allied deployed in Romania (in terms of contribution to the HNS) – must be configured and equipped to allow generation of combat missions by providing: (1) Aircraft operating surface or ground aircraft operations (need to fulfill certain conditions relating to the status and the technical characteristics of the runways, taxiways regarding their size, to allow both fighters and large transport aircraft (airlift and cargo), such as C-17 Globemaster, C-5 Galaxy, etc.); (2) The necessary technical areas and surfaces for inspections, maintenance, testing and evaluation or repair of aircraft and associated equipment; (3) Logistical support areas for the storage and dispensing of materials, equipment, consumables (i.e., fuels, oils, and lubricants) along with ground vehicle operations, maintenance, and repair.; (4) Headquarters and administrative facilities for command and personnel support: (5) Communications and information systems support; (6) Food service and dining facilities; (7) Industrial areas to include utility systems and facilities; (8) Medical facilities; (9) Security and fire protection facilities; and (10) Unaccompanied and accompanied housing.[13]

From an operational perspective, the air bases infrastructure should allow carrying out different activities, related to weapon systems operated within the base or the nature of supporting activities in accordance with the principle of specialization. Relating to this criterion, airbases will be for: (a) *generation of combat missions* independently performed or as part of an air campaign; (b) *generation of offensive and defensive operations and electronic warfare support* provision of information or functions associated with C2; (c) *providing highly specialized technical support* necessary on maintenance activity, repair, research and development; (d) *the provision of medical support* through the use of skills and capabilities held, such as aero-medical evacuation; (e) *support the processes of training, flight training and the education*; (f) *testing and evaluation of air platforms, weapons* and systems of weapons, respectively associated functions C2.

The air bases and infrastructure will be the capability by which the Romanian Air Force will generate combat power through providing the carrying out missions for engaging hostile forces, but also exercising control over resources. The dependence thus created between missions and the infrastructure support offers the infrastructure quality of center of gravity, thus making it a target to be neutralized for enemies, which requires development of protection plans from peacetime. However, it is not sufficient that air bases and facilities to be only able to withstand air strikes or ground. They must be able to ensure prolonged and concentrated combat missions against the enemy.

Conflict situation such as the one in Libya in 2011 (*Unified Protector*) – even if it was not of a very large scale – showed shortcomings that causes the execution of air operations performed on the air bases located far away from the conflict zone. But their presence becomes mandatory both for long campaigns, to meet operational requirements that such a campaign involved (tempo of operations, availability of fighter and ground attack aircrafts, transport and air refueling platforms, ensuring operations maintenance, providing search and rescue service etc.) and where the military operation involves the participation of ground forces, which implies a different set of activities (from airlift of forces and equipment in theater and ending with providing logistics, medical, etc.).

From the same expeditionary forces perspective, for the operation of these bases in optimal conditions necessary to generate the combat capabilities in theater, it is necessary deployment/ redeployment and development of facilities in order to support forces in a timely and effective manner. This implies the existence of previously established procedures and agreements: *"set points of entry and departure, overflight authorization, authorization to use*

[13] US Air Force, *Air Force Doctrine Document 2-4.4 – Bases, Infrastrastructure and Facilities* , 13 November 1999, p. 14.

radio frequencies, air traffic control, diplomatic approval on air bases operation, agreements on access facilities, Coalition contracting procedures, connectivity, force protection, assessment/ site-survey, handling and storage of explosives, ammunition and weapons etc."[14].

The above statements should be understood in terms of processes and standards that once met, will enable the deployment of military operations in joint and multinational environment, thus each weapon, aircraft or ground equipment, operational capability of the Alliance can be connected to a hub or common network, enabling actional synergy for NATO member states forces, regardless of the battlefield. The aim is to achieve interoperability, which can be ensured by common standards and procedures in terms of organizational and system compatibility.

3. Operational requirements imposed on aircraft and weapons systems from the equipment of the future air forces of Romania

To establish the operational requirements of aircraft that will equip the future air forces of Romania, it is appropriate to use *the same approach for analyzing the supervenience relationships between the physical and the operational* features associated to the mission.

From the perspective of actional expression, the air forces, through their unique attributes, will remain the only category of forces that can cover the full spectrum of missions, from traditional offensive and defensive ones, of force application - in national defense space operations or of the NATO integrated space - to the expeditionary ones, namely those performed in support of the work of organizations such as the UN, OSCE etc, for the maintenance and enforcement of peace, humanitarian assistance or imposing sanctions.

Develop innovative concepts in the Alliance, and the experience of NATO military involvement in conflicts in the past two decades should be the foundation of procurement processes and of the integration of new air platforms and weapon systems in the weapons inventory of the Romanian Air Force. In order to allow the full range of missions mentioned above, it is necessary that the air force have a varied inventory of air platforms (fighter, bombing-fighter aircraft, cargo and airlift aircraft for transport of forces and materials in theaters, air refueling tank planes, flying school aircraft for training, attack helicopters, medical evacuation, search and rescue and combat search and rescue helicopters (MEDEVAC, CSAR).

Such an inventory would allow the implementation of new concepts in the Romanian Air Force, as well as *network centric operation and effect-based operations* in terms of the impact generated on the assigned objectives. Conceptual reorientation at the level of NATO decision makers regarding operations planning, from those threat and platforms-centered type, to the ones centered around adaptive capability and effect-based would be thus validated, by providing commanders with a full arsenal of aerial platforms, weapons and weapons systems, of which they can select depending on the desired effects in the theater.

Regarding combat aircraft for providing kinetic effects on enemies - air campaigns carried out from the end of the Cold War to the present have demonstrated the need to have some platforms to be able to act in increasingly complex and restrictive current combat theaters, issue which involves holding features that allow them both discovery and fighting opponents and own protection against multiple threats from the air and the ground. On the other hand, the limitations imposed by the rules of engagement, and the need to conduct operations to eliminate opponents in urban areas in close proximity to civilian non-combatants etc. determine inclusion in the arsenal of aircraft possessing distinct characteristics (speed, range, acquisition and maintenance costs, but also the possibility of

[14] Michael W.Lamb, *Operations Allied Force – Golden Nuggets for Future Campaigns*, BiblioScholars, 2012, p. 17.

integrating intelligent lethal and non-lethal ammunition, network operating capability to use functions that allow identification and target designation in the shortest possible time, etc.) that can determine the desired effects in the theater without causing destruction and collateral damage.

Theaters where aerial platforms will evolve in the future are likely to experience massive infusion of new generation weapons systems, possessing greatly improved characteristics of both self-protection and survival and enforcement capabilities of decisive strikes, while the integration of particularly performing sensors contribute to the permeability and transparency of the operational environment. This foreshadowed reality requires the development of systems which, once integrated in aircraft, enable the survival and execution of suppression of enemy air defenses missions (SEAD).

In the same direction, due to multiple threats in theaters, it is required that we integrate weapons and avionics systems on aircraft enabling them during a single mission to execute multiple actions, consisting of hitting targets and distinct targets in different operating environments by launching suitable weapons and ammunition. For it is also required, along with the possibility of carrying a wide range of weapons (air-to-air, air-to-ground, intended for strikes against surface vessels, radars etc.), and the possibility of under-wings carrying equipment (pod-type) which hold certain distinct functions, enabling *the launch of precision weapons, accurate discrimination and engagement of priority targets, high performance in very low visibility flights, day or night by using terrain-following radar* etc.

From the perspective of the use of *weapons and ammunition*, is required a standardization and compatibility, both at the technical level of the aircraft regarding the under-wings weaponry loading/ carrying capabilities (missiles, bombs, cannon fire, etc.), which is particularly important in the context of air operations, by reducing the arming time, avoiding carrying out separate and parallel processes for assembly of missiles, bombs, etc., which determines both maintaining of a high tempo of combat operations and making processes efficient.

Other requirements impose the integration of equipment (communications systems resistant to jamming, identification systems, etc.) that provides interoperability with NATO allies military forces. Thus the on board air platforms arrangement of the fighting equipment *Link-16* - a military tactical data exchange network used by the US and NATO, but also other countries such as Sweden and Japan - facilitates exchange of data regarding the battlefield (the arrangement of the allied and enemy aircraft, ships and ground forces units, etc.) in real time, automatically and at great distances, with the Allied platforms that have integrated onboard this capacity (most aerial platforms of NATO member states, including AWACS platforms, some carriers and ships of the Alliance, the missile defense systems, command and control elements etc.).

Summarizing the above requirements, we have outlined the operational profile of the future Romanian Air Force fighter planes, specific to multirole, modern, 4th generation planes, compatible with NATO states, able to execute tasks in a complex, unpredictable environment, characterized by multiple risks and asymmetries.

Synthesized, these requirements include: (1) *maximum effectiveness* in the modern battlefield conditions; (2) *increased capacity to survive* in hostile environments, under electronic warfare; (3) *flexibility in the execution of the full range of missions*, allowing reconfiguration / change of mission during flight; (4) *generating a large number of sorties per unit of time* by reducing the time required for restoring the ability to fly and fight; (5) *low operating and maintenance cost* during usage; (6) *enhanced flight autonomy*, achieved by lower fuel consumption; (7) *the ability of loading/ carrying multiple weapons* and ammunition (air-to-air, air-to-ship, jamming systems, etc.) in a large amount; (8) *open architecture* that provide opportunities for further modernization, special flying and

maneuvering qualities (expressed by supersonic speeds at any altitude, very good maneuvering qualities, unrestricted ground and flight operation, flight refueling system, reducing the pilot's tasks, efficient resource use of the aircraft, good takeoff / landing features etc); (9) *the integration of compatible systems and equipment* with the Allies.

To perform expeditionary missions, the Air Force will have to operate *airlift and cargo platforms*, as critical capabilities enablers in support of air operations through the air move of troops, equipment, weapons systems, etc. to optimal locations within the NATO Area of Responsibility (AOR), or beyond. Currently, Alliance military forces are using aircraft for strategic transport C-17 and C-5 (UK holds eight C-17, Canada has 4 C-17, and 10 NATO members have access to a separate group of three C-17, known as the *Strategic Airlift Capability - SAC)*.

Similar with combat aircraft, they must satisfy a set of operational requirements related to: (1) *effectiveness in complex operating environments*; (2) *efficiency in relation to operating costs***,** *maintenance*, etc.; (3) *ability to survive in hostile environments*; (4) *high flying autonomy*; (5) *high loading capacity*; (6) *integration of onboard navigation equipment, modern radio navigation that allows flight in all weather conditions, day and night*; (7) *the ability to take off and land from/ to austere, small runways*; (8) *open architecture*, allowing subsequent upgrading; and (9) *systems compatible* with other NATO and allies platforms.

Regarding *ground-based air defense systems* (*GBAD*) of the air forces of NATO member states (GBAD), their importance is even greater in the future conflicts because, under the threat conditions outlined above, the striking capabilities of potential adversaries will see significant development. Their development, in order to be adjusted to operational needs, will be an important element of combat, but also a major deterrent in case of a virtual aggression against the security of NATO airspace.

Conclusions

New missions undertaken by the Alliance, to which Romania takes part, being in a constant redefinition and adaptation due to external factors, have led to a set of parameters associated with both operational structures, and also with infrastructure and air platforms from own inventory, understood from the perspective of the goals pursued (missions, roles).

Meeting these requirements involve – along with issues related doctrines, force generation, instruction and training – and technical issues associated to equipment, weapons and ammunition, weapon systems, infrastructure elements, respectively associated to processes (acquisition, procurement and equipment). Thus, each of these capabilities implies the existence of specialized infrastructure elements, allowing the core activity and processes for the exercise of roles and mission execution.

This is particularly important in system design and integration of collective defense infrastructure operational needs adjusted accordingly, especially since the degree of security environment complexity is constantly changing, causing a new hybrid threats as expression, hard to to predict and combat. It is not enough just holding last generation modern weapons systems, of the latest technologies and equipment if they are not supported by an adequate system of C2 on the ground on one hand, and the logistics infrastructure to ensure both operation and maintenance effectively and efficiently.

Although the development of platforms capable of projecting power globally by running missions is a continuous process, reducing the need for a system of forward operating air bases, air campaigns have emphasized the importance of contemporary existence of such bases, *"representing a fundamental requirement for success in operations expeditionary*

forces"[15]. Lack of an sufficient number of bases or their crews not only creates pressure (due to increasing complexity in the execution of very long flight, the need to implement a large number of air refueling and then to execute the attack on targets etc.), but also the planning factors and logistics systems.

Romania has a valuable infrastructure and facilities – which are made available to the Alliance since the pre-accession – consisting, along with airports, ports, terminals, railways, deposits and medical facilities, maintenance, logistics and communications. Regarding the degree of functionality and their development, modernization workflows continued to achieve standards set in the North Atlantic Alliance.

Along with quantitative requirements on the physical existence of a sufficient number of operating bases, qualitative requirements must be met to allow execution of air operations in terms of generating support operations such as restoring its capacity to fight, providing the necessary aircraft and equipment logistics and maintenance execution, technical and personnel protection, medical support, personnel feeding etc.

Future conflicts will involve the participation of different actors, organized in various alliances, *"nations being inclined to pursue the unilateral operations, and other form of coalition made up of a broad range of partners with different capacities"*[16], which implies a new understanding at infrastructure level regarding the system compatibility, which is not enough to satisfy only the equipment and weapon systems of NATO military forces, but also those of potential coalition partners.

The future assuming of a variety of new missions and roles, carried out with allies, such as those deployed in support of UN and other organizations, involves equipping the Air Force with an inventory that meet this level of involvement, consisting of various, specialized air platforms, from the ones used for strike and power enforcement, continuing with the ones designed to ensure global mobility and support, search, rescue and evacuation, etc. Their features should allow evolution and survival in complex operation theaters, operation on poor air bases, with rudimentary, small runways etc. From another perspective, because of the joint and multinational military features of the conduct of Alliance military operations, NATO member states aerial platforms must have compatible communication, identification systems etc. to achieve interoperability, thus operating in an effective, efficient, and safe manner.

BIBLIOGRAPHY:

1. Duşa, Mircea, *Bilanţul MapN pe 2014,* Ministerul Apărării Naţionale, Bucureşti, 10 martie 2015, TVRNEWS.
2. Greanleaf, Jason R, *The Air War in Libya*, în *Air & Space Power Journal*, martie-aprilie 2013
3. Lamb, Michael W., *Operations Allied Force – Golden Nuggets for Future Campaigns*, BiblioScholar, US, 11 September 2012
4. Ministerul Apărării Naţionale, *Carta Albă a Apărării*, Bucureşti, 2011
5. Ministerul Apărării Naţionale, *Planul Strategic al Ministerului Apărării Naţionale 2010-2013*, Bucureşti, 2010
6. Ministerul Apărării Naţionale, *România – NATO, Primii zece ani*, 2014
7. Ministerul Apărării Naţionale, *Strategia de transformare a Armatei României*, Bucureşti, 2007

[15] Ibidem.
[16] Jason R.Greenleaf, *The Air War in Libya*, în *Air & Space Power Journal*, martie-aprilie 2013, pag.44.

8. NATO Infrastructure Committee, *50 Years of Infrastructure – NATO Security Investment Programme is the Sharing of Roles, Risks, Responsibilities, Costs and Benefits,* 2001
9. Orzeaţă, Mihail, *Globalization, Crises and World Security*, LAP LAMBERT, Academic Publishing, Germany, 2013
10. US Air Force, *Air Force Doctrine Document 2-4.4 – Bases, Infrastrastructure and Facilities,* 13 November 1999
11. www.nato.int

TENDENCIES AND CONCEPTS IN LAND FORCES MODERNIZATION

Cristinel Dumitru COLIBABA
PhD student, 280th Mechanized Infantry Battalion
e-mail: cristicolibaba@yahoo.com

Abstract: *To be competitive and to operate effectively in the face of new risks and threats generated by developments in contemporary operational environment ground forces must adapt continuously. Resilience lies in implementing a modernization and transformation plan to provide long-term vision to support the development effort of capabilities and forces to be successful in joint space battle.*

Key words: *adapt, land forces, operational environment, transformation, system*

Introduction

History has always shown that armies that are willing to continually adapt are successful in battle, fact especially true today, when it is possible to deal with unconventional adversaries who has a greater capacity to adapt, not restricted by the bureaucratic process or moral constraints.

To avoid adopting a reactive attitude against an opponent always been one step ahead of our plan is required to implement a long-term transformation plan of the armed forces containing changes demanded by the evolving capabilities and future operational context. This plan should be the center of gravity of the process of modernization and transformation of the Romanian Armed Forces and provide a clear vision of the land forces future in order to support efforts in developing the forces and capabilities.

This plan ensures constituents, people, equipment and technology that will allow ground forces to achieve victory in joint battle space of the future and also can identify issues that need deeper investigation, experimentation and analysis.

Proposed approach must be the starting point in describing the operational environment and establishing principles to be observed in generating future force structure, subsequently identifying concepts and tactical requirements necessary to effectively manage future conflicts.

1. Operational context

Even if the future cannot be predicted and uncertainty will be the dominant feature of the operational environment in which land forces operate, can be determined relatively stable trends that may guide with sufficient clarity modernization efforts.

A starting point is the fundamental mission of the Romanian Army, which consists of "Defend the national interests of Romania in accordance with constitutional democracy and the democratic and civilian control over the armed forces. Army must be prepared to prevent, deter and counteract a possible armed aggression against Romania and its allies"[1] as well as general tasks stipulated in the Defense White Paper, namely:

[1] Ministerul Apărării Naţionale, *Carta albă a apărării*, Bucureşti, 2013, p. 25.

- Contributing to the security of Romania in peacetime;
- The protection of sovereignty and territorial integrity of Romania;
- Participation in the defense of its allies within NATO and the EU;
- Promoting regional and global stability, including through defense diplomacy;
- Support central and local public authorities in emergencies, for assistance to the population and managing the consequences of disasters.

To achieve these missions is necessary to use modern concepts of operational planning, one of them being "adaptive campaign" which contains five lines of independent operations but which can complement each other: Joint Ground Fight, Population Protection, Information operations, Support Local Population, and Development Local Capabilities. Future land forces need to be optimized for first-line of operations, although it will have the ability to participate, if necessary, in the operations of others lines, because carrying the battle and safety they offer is a prerequisite for execution of other lines of operations.

Given the complexity of the operational environment, land forces will be key to successful manage the effort in the five lines of operations, in the right place at the right time, with the following principles:

1. Flexibility - the ability to maintain efficiency over the entire range of tasks, situations and circumstances, through a line of operation;
2. Agility – the ability to manage dynamic, in time and space, effort capacity along all lines of operations;
3. Resistance - the ability to withstand losses, damage and delay capability to maintain essential levels of key functions;
4. Responsiveness – the ability to quickly identify and subsequently effectively respond to new threats and opportunities within a line of operation;
5. Robustness - ability to generate and sustain an optimum force level depending on population density and opponents capabilities, thus achieving adequate control of the operational environment to manage uncertainty and act along the five lines of operations.

Another aspect that should be taken into consideration in designing the future force structure is the ability to operate in urban areas, including humanitarian assistance and reconstruction operations, and also operations in which opponent deliberately adopts the tactic of "hiding among population ". In fulfillment of all tasks and duties, the soldiers of the land forces of the future should be able to effectively engage the local population in order to influence perceptions and behavior.

Technology is another element that will have an important impact on operational environment and although technological advantage will remain a key component of military effectiveness, its impact will depend largely on how it is used and the skills of those who use it.

From the point of view of potential threats that land forces will face it is said that nature of adversary may vary from one major, even if at the moment, according to the National Defense Strategy, the possibility of a traditional interstate conflict appears to be minimal for Romania, a series of irregular forces ad hoc constitute may execute actions across the whole spectrum of conflict. Opponents that land forces is possible to face in the future will be adaptable and will change operational approach in the light of experience, the most dangerous course of action is an opponent who would be able to coordinate the execution of a multi-dimensional campaign, attacking simultaneously in physical, informational and moral dimensions.

Given the nature of future type of conflict, it is likely that a wide range of activities within the battle space to be carried simultaneously, many of these being the traditional boundary between military and civilian responsibilities, including law enforcement actions, disaster relief and developing local capabilities. Thus, fewer future security challenges will be successfully solved only by military force and more than that, taking into account the impact

of globalization and increasing interconnectivity of countries, land forces will likely act as part of a joint force, interagency, intergovernmental or multinationals.

The human dimension is another aspect that must be taken seriously because, as always, success of the land forces will depend on its soldier's abilities, specifying that in the future operations tactical actions of each soldier and their consequences can have strategic importance. Given the increased likelihood of a thorough examination of the media and the public in general will become an imperative operational transparency and adherence to the highest ethical values will be crucial. Furthermore complex decision-making skills will be critical for soldiers of all levels.

2. Tactical level consideration

The future land force will be represented by a system of systems that will include different types of forces, different levels of readiness, training, equipment and personnel are integrated to achieve operational effectiveness. Each element of the system has different characteristics and capabilities so that to support proper development of these elements is necessary to use a new concept evolved from battlefield operating systems and warfighting functions thereafter called primary land integrated systems. The difference between the two concepts is that while warfighting functions are concentrated on orchestrating effects, primary land integrated system is a comprehensive approach that focuses on development and integration of capabilities which allow the effects on the battlefield and contains the following systems:

- Soldier as a system;
- Combat system;
- Special operations system;
- Combat support system;
- Logistic support system
- The system of command, control and communications (C3).

The soldier as a system. A first primary system is "soldier as a system" concept having no intention to dehumanize the soldier, but to emphasize the importance of the individual in future structure of land forces. Considering the soldier as a distinct system, ensures that everything soldiers learn, every action it performs, everything employs, transports, and consumes work together as an integrated system. From the point of view of the human dimension that individuals need to be prepared to execute specific land forces operations by developing the soldier physical components, psychological, social, intellectual and moral.

The *combat system*[2] will be required to establish and maintain security in environments characterized by violence, uncertainty, complexity and chaos and consists of soldiers and terrestrial mobile platforms, elements that provide the fight ability to a joint force, in contact with the opponent regardless of terrain and tactical actions in the entire spectrum of conflict.

The *special operations system* contains forces capable of performing specialized operations by individuals and teams carefully selected, trained and prepared with the benefit of an attitude capable of producing creative solutions beyond conventional approaches. The main advantage of this system is the ability to execute the full spectrum operations based on the unique ability to solve problems through which to achieve operational and strategic effects.

The Special Operations system is constructed around the core-means-methods capability design parameters:

[2] Key Combat System Considerations: Integration, Interoperability, Future-Proofing, Simulation, Adaptive Acquisition.

- Core. The core of Special Operations capabilities is outstanding people, embodying the highest possible quality of intellectual and physical capital. This core is the centre of gravity of all Special Operations activities and is the fundamental equity which must be protected and developed. The skills, profiles and diversity of the Special Forces will expand significantly in non-traditional ways and this increased diversity will enable the Special Operations capability.

- Means. Highly networked relationships and strategic partnerships are critical to an adaptable Special Operations force posture and appropriate positioning. Innovative technology, in the hands of outstanding people and used in unconventional ways, is a critical enabler of Special Operations.

- Methods. All Special Operations are underpinned by unconventional approaches, the element of surprise, and the ability to shape, influence and strike adversaries when and where they least expect. This drives the requirement for innovative, unorthodox personnel and equipment and the ability to tailor effects with precision and discrimination. The Special Operations organization must seek to be versatile, agile and adaptable.

Combat support system is a set of sub-critical systems to achieve and maintain freedom of action and to ensure capacity multiplied by combat support operations, namely: force protection, battle space awareness, information operations, mobility, joint fires, air and missile defense, maneuver support, protection against improvised explosive devices and CBRN defense.

Force protection involves coordinated action to counteract in time and space and limiting risks and threats, in order to ensure an operational environment where commanders have freedom of maneuver. To ensure the protection of future land forces need a balanced set of measures assets, liabilities and recovery offering flexibility and agility to respond effectively to new circumstances while maintaining the ability to perform the tasks entrusted.

Knowing the battle space provides estimates developing relevant, accurate, comprehensive and in short time to allow the successful application of combat power, protect the force and fulfill the mission and includes in turn sub-system information, surveillance, target acquisition and reconnaissance (ISTAR) and sub-system electronic warfare[3].

The ISTAR system must be able to perform the following functions:

- Command-directed Prioritization. The commander must set and prioritize his Commander's Critical Information Requirements (CCIR) in order to drive and direct the collection effort.

- Mission Management. Mission management must be centrally coordinated in order to enable the acquisition, integration and exploitation of real time information from across the full spectrum of sensors to support decision-makers at every level.

- Collection. Collection is the exploitation of networked Sensors, Sources and Agencies (SANDA) from which information and intelligence feeds are drawn.

- Analysis. Analysis is the processing phase of the ISTAR cycle in which information is reviewed in order to provide a fused multi-intelligence product that answers the CCIR.

- Exploitation. Exploitation ensures that the actionable intelligence is the highest grade that can be gleaned from exploited documents, media and human sources to inform the evolution of CCIRs.

- Dissemination. Dissemination involves the timely passing of intelligence in an appropriate form and by any suitable means to decision-makers.

[3] Electronic Warfare system contributes to a range of effects within the battle space and includes: Electronic Support, Electronic Attack, and Electronic Protection.

Information operations will be an important activity in the future given that the information environment[4] will significantly affect the future operations of rapid enforcement organizations and global networks of circulation of information. Therefore, this sub-system must ensure that information held by ground forces offers an advantage over the opponent by exploiting all available means, including engaging communities, international forums and media.

Mobility is another key feature of future land forces and is primarily aimed at dislocation of fighting elements close to the objectives where they can disembark in relative safety and execute the assault. This sub-system comprises an optimized firepower, mobility and protection and is able to support large-scale operations in time and space.

For effective execution of fire support is fundamental for this sub-system the ability to plan, coordinate, prioritize and achieve precise and controlled effects on extensive areas in support of land forces. Its goal is to engage threats while taking all the measures for avoiding fratricide and collateral damage and ensure the ability to be integrated at the lowest level with allies to achieve joint effects within multinational coalitions.

Sub-system missile and air defense will be composed of ground-to-air weapons systems to be complementary components of aerial surveillance thus ensuring an optimum level of protection against a wide range of possible threats, such as airplanes and helicopters, unmanned aerial systems, artillery weapons and missile systems.

Sub-maneuver support system will incorporate two main concepts:

- Mobility assault, which consists in making the transition actions and removal of barriers and execution breaches to create favorable conditions for maneuver combat forces in any ground, before, during and after the contact with the opponent.

- Risk management, which consists of specialized capabilities to minimize future battle space hazards, including asymmetric attacks with explosives and CBRN.

Defending against attacks with improvised explosive devices are based on a multidisciplinary approach, targeting and attack at beginning the networks to prevent placement of such devices, and where this is not successful will move to neutralize the device.

CBRN defense will focus on ensuring protection against threats both conventional and those improvised. To counter conventional threats this sub-system will continue to rely on data collection and warning information and employment, on joint fire support for execution of attacks and engineering support for devices neutralization , while in the case of non-conventional threats should be used a similar procedure as for CIED defense.

The *logistic support* is a key element in the modernization approach and land forces must be able to provide resources and essential services in a proactive manner through the effective use of network and staff available on hand.

It consists in turn of a series of sub-critical systems, such as:

- Maintenance sub-system;
- Health Sub-system;
- Service campaign sub-system.

The command, control and communications is another decisive factor for the success of land forces in the future battle space and should be able to adapt to the operating environment while exploiting the available capabilities effectively. This is a new concept called "control system, adaptive control and communications" containing people (commanders and staff personnel), organizations and networks, all of which main characteristic resilience.

[4] The information environment is the aggregate of individuals, organizations, their societal and cultural patterns and the systems that collect, process, disseminate or act on their information.

Conclusions

The military system evolves and its components are becoming increasingly integrated and interlinked, so it is essential to identify those capabilities that must be kept, those that have to give those who can redistribute to other system elements defense.

Following the completion of the present approach can establish some guidelines of the process of modernization and transformation of the army, namely:

- Execution of battle against an opponent to be credible remains the foundation on which to plan force structure;
- Balanced development of structures for maneuver and support to be able to contribute to national defense and national interests;
- Implementation of strategic concepts, operational and tactical us to increase the efficiency of planning and execution of the full range of missions;
- Developing the capacity to act in land forces met and multinational framework;
- Develop a force that is adept of efficiency and effectiveness philosophy by exploiting emerging technologies.

Acknowledgements:

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. AUS Departement of Defence, *Campania adaptativă. Conceptul viitor de operare a forţelor terestre*, Canberra, 2009;
2. Carta albă a apărării, Bucureşti, 2013;
3. Land warfare development centre, *The Army Objective Force 2030*, 2011;
4. Strategia naţională de apărare a ţării, Bucureşti, 2008;
5. US JFCOM, *Mediul operaţional întrunit. Lumea până în 2030 şi mai departe*, 2006.

CYBERSCAPE: CYBERSECURITY AS A FIELD FOR CONTEMPORARY CONFRONTATION

Manuel José GAZAPO LAPAYESE
PhD Candidate. Master in International Affairs (Universidad Pontificia Comillas).
Chief Manager of International Security Observatory, Researcher at Universidad Politécnica de Madrid., Spain, e-mail: m.gazapo.lapayese@hotmail.com,
internationalsecurityobservatory@protonmail.com

Abstract: *Cyberspace should not be regarded as an aseptic, abstract dimension detached from human beings; quite the opposite, it is a characteristically nebulous, rhizomatic, open, multiple environment for human relations. These traits lead to an understanding that the operation of the contemporary world is in close relationship with the evolution of cyberspace and of cybersecurity mechanisms. Due to this, cyberspace demands increasingly greater attention from the international community.*

Cyberspace has arisen as a new space for -Internet-based- global confrontation and has therefore inherited its conflicts from the more traditional dimensions: land, sea, air and space. Because of this, an analysis of cyberspace in this international conference was called for, discussing its distinctive characteristics, the scope of cyberattacks and the range of solutions that can be put into practice in order to respond to these new and significant threats.

Keywords: *Cybersecurity, cyberspace, 'cyberscape', cyberattacks, resilience, threats, vulnerabilities, solutions.*

Introduction

Within the STRATEGIES XXI Conference: 'The Complex and Dynamic Nature of the Security Environment', we believe that it is highly interesting to develop an understanding of cyberspace as the new landscape –the new field for confrontation– on which an increasingly greater number of security operations are being carried out at present.

In that vein, by joining the terms *landscape* and *cyberspace* we have coined the concept of 'cyberscape', intended to describe the complex landscape of the Internet in the present day. If 'cyberscape' is defined as the landscape of cyberspace, as a contemporary battleground where security is an as yet unresolved issue, particular attention will have to be paid to the risks and threats that this new landscape of conflict brings about. Therefore, this international communication will try to address the following three tasks:

-Analysing the distinct characteristics of cyberspace; understanding the reasons why conflicts are transported to cyberspace, as well as the scope of cyberattacks.

-Becoming aware of the destructive power of cyberattacks by discussing some of the most significant cases, such as the Russia-Estonia conflict, the effect of the Stuxnet virus in Iran, WikiLeaks and the massive cyberattack known as Red October.

-Understanding the 'cyberscape' as a new strategic chessboard, while discussing the lack of consensus behind the concept of 'use of force', system vulnerabilities and possible solutions.

1. Cyberspace and cyberattacks

If we seek to analyse the distinctive characteristics of cyberspace and to understand the reasons behind the extrapolation of conflicts to cyberspace as well as the scope of cyberattacks, it is vital to understand that the scenario we are facing is completely different from anything previously known to us.

1.1 Understanding cyberspace

Conflicts in cyberspace are fundamentally open and asymmetrical in nature, since the weaker party is capable of attacking a conventionally stronger opponent. Due to this, it can be argued that cyberweapons are revolutionising international relations and, consequently, warfare: any unprotected computer, system or network is a cyberweapon waiting to be loaded and used. Until we accept this premise, we are all at risk.

By its own nature, cyberspace enables any state, institution or individual to gain access to it regardless of its geographical, economic, social or logistical situation. Thus, some of the main causes for which conflicts are transported to cyberspace are the economic advantages, operational capacity and operative flexibility of the digital dimension, regardless of whether the actor is a state, a corporation, a criminal organisation or an individual hacker. This reveals the low cost of operating within it as one of the causes that make cyberspace an attractive battleground. Meanwhile, the destructive capacity and reliability of a properly designed and coordinated cyberattack can make its effect devastating, to the point of paralysing a state or sending it into digital blackout.

As well as the former, the anonymity of cyberspace and the difficulty in reliably identifying culprits are key reasons behind the steady increase in attacks within cyberspace. A recent news article gives a clear example, stating that "95% of cybercrime goes unpunished […] This is of great importance at a national and international level due to the danger it presents to citizens, the economy and critical infrastructures" [1]. The impossibility of curtailing the fraudulent use of the Internet through International Law –for any terminal with Internet access is a potential enemy– has made cyberattack prevention a characteristically difficult task, for "there will always be a possibility that anybody, from their own living room, will generate and spread a piece of code with catastrophic consequences" [2].

Here, we are witnessing a double phenomenon: on one hand, the externalisation of cybersecurity, which is a delicate issue since it complexifies the map of present-day cybersecurity, drawing attention to the fundamental need for global cooperation between the public and private sectors in this new scenario. On the other, the outsourcing of state security to private contractors which, while reducing costs significantly, also poses a great threat to national security due to the fact that there cannot be a complete certainty that these contractors will follow and uphold all the requirements implicit in managing a state's security and their citizens'.

In light of the previous facts, governments will have to be prepared to face threats to critical infrastructures such as industry, nuclear and conventional power stations, satellites and submarine cables. This is a vital issue both for the security of governments and their citizens, and for the stability and development of corporations at a global scale.

---

[1] Duva, J. (2014) "El 95% de los ciberdelitos cometidos quedan impunes" *El País.* [Online] 4 May 2014. Available at: <http://politica.elpais.com/politica/2014/05/03/actualidad/1399117342_852720.html> [Consulted 11 May 2014]

[2] López, J. (2012) "La evolución del conflicto hacia un nuevo escenario". in *El ciberespacio. Nuevo escenario de confrontación.* Ed. Ministerio de Defensa. Madrid: Ministerio de Defensa, pp. 117-166.

1.2 Understanding cyberattacks

In the current international context we can see how cyberattacks can affect computers as well as mobile phones and wireless computer networks. There is no limit or barrier to prevent cyberattacks from penetrating any entity with an Internet connection. This means that cyberattacks use security loopholes in information technologies to access terminals and then go on to copy, delete or rewrite the victims' information; for this, they take advantage of the vulnerabilities shown by most current cyberstructures such as, for example, social networks.

Attackers can be classified according to multiple categories, such as authorship or motivation. It is through authorship that we can best draw up a classification of attackers allowing for a better legibility of cyberspace as a new scenario for confrontation: among other actors or entities, we can identify states and corporations on one hand, and terrorist groups and criminal organisations on the other, as the culprits behind most cyberattacks.

This helps us understand how, in the near future, confrontations in the virtual world will have much more damaging effects than they have at present, even though the fact that states lie behind many cyberattacks makes their identification and attribution easier:

"*Today, in cyberspace, where attacks can launch in milliseconds, a nation might not have enough time to detect an attack and mount a defense*"[3].

All in all, against the unstoppable metamorphosis of cyberattacks and the unpredictable direction of their evolution, it is crucial to stop to think on how much our dependence on Internet usage can ultimately jeopardise our security.

2. The destructive power of cyberattacks

Real-world conflicts, which we have been witnessing to the present day, now have their continuation in the virtual world of cyberspace. This indisputable reality carries behind it the idea that the 21st-century state's sovereignty does not only reach its territory, maritime space and airspace, but its electronic infrastructure and cyberspace as well. As the second stated goal of this international communication was raising awareness of the destructive power of cyberattacks, we will proceed with a discussion of the most relevant cases of conflicts at the digital level to this day:

2.1 Russia-Estonia cyberconflicts: the real-virtual interconnection

The 2007 Estonian incident served to highlight the interconnection between the real and virtual worlds: an ostensibly irrelevant political decision –the relocation of a World War II memorial – not only led to social unrest and protests, but also triggered a cyberattack causing the complete collapse of the system at a national level.

2.2 WikiLeaks: the lack of cybersecurity

Another case where cybersecurity has been a key element is WikiLeaks. The leakages and information theft that took place reveal how governments' cybersecurity systems –in this case, the algorithms protecting the files of the US Government– were not, and still are not, totally secure and impenetrable, for they are continually under siege from hackers or actors with an interest in breaching their barriers and accessing the information behind them.

[3] Nakashima, E. (2013) "In cyberwarfare, rules of engagement still hard to define". *The Washington Post.* 10 March 2013. Available at: <http://www.washingtonpost. com/world/national-security/in-cyberwarfare-rules-of-engagement-still-hard-to-define/2 013/03/10/0442507c-88da-11e2-9d71-f0feafdd1394_story.html> [Consulted 2 May 2014]

2.3 Iran and the Stuxnet virus

In 2010, a sophisticated computer virus known as Stuxnet paralysed all the control systems of Iranian nuclear power stations. The strength and complexity of Stuxnet, as well as its effectiveness, have led many experts to suggest that it almost certainly must have been designed by a state. Additionally, the Flame virus –a morphing of Stuxnet– has been considered by many experts to be the first global-level cyberweapon. Many countries' intelligence services have classified the Stuxnet virus and its evolution known as Flame as the first 'cyber-nuclear weapon', due to its high strength and complex design: "Flame is a highly sophisticated, malicious program that is actively being used as a cyberweapon to target entities in several countries […] Flame can easily be described as one of the most complex threats ever discovered. It's big and incredibly sophisticated. It pretty much redefines the notion of cyber war and cyber espionage"[4].

2.4 The Red October cyberattack, 2013

We will conclude this part by citing briefly the massive cyberattack known as Red October. In 2013, the cybersecurity corporation Kaspersky Labs informed the BBC that they had discovered a new, massive global cyber-espionage operation with an extremely high capacity for destruction: "Since 2007 it had been attacking governmental institutions from various countries such as embassies, nuclear research centres and organisms linked to the gas and oil industries […] It was designed to steal encrypted files and was even able to recover those which had already been deleted […] its main goal were Cryptofiler files, based on an encryption technique used by institutions such as NATO and EU to protect their most sensitive communications". [5]

The idea that transpires from these declarations is that all countries without exception should begin promoting collective actions to prevent this kind of attacks, as has been done for nuclear, biological and chemical weapons –for the possibility of suffering a cyberattack can put any country's national security at risk: "a cyber-attack perpetrated by nation-states or violent extremist groups could be as destructive as the terrorist attack on 9/11"[6].

3. Cyberspace: new rules, new vulnerabilities, new solutions

The third and last goal of this communication, titled 'Cyberscape: cybersecurity as a field for contemporary confrontation', is understanding the 'cyberscape' as a new strategic chessboard. For this, a reflection is needed on the lack of consensus on the use of force, the system's vulnerabilities and possible solutions:

3.1 New board, new rules

As announced in the beginning, it is crucial to reflect on to what extent our dependence on Internet usage can put our security at risk. For instance, both governmental and non-governmental infrastructures on a global scale are now characterised by interdependence and Internet-based interconnection: such an ease of contact and information exchange between actors through the Internet may initially lead us to think that there only are

---

[4] Kaspersky Lab. (2012) "Flame…The latest cyberattack. What are the risks -and is protection necessary for you?" in *Kaspersky Lab Corporate News* [Online] Available at: <http://www.kaspersky-sea.com/flame/> [Consulted 2 March 2015]

[5] Lee, D. (2013) "Descubren en Rusia masivo ciberataque mundial". *BBC.* [Online] 15 January 2013. Available at: <http://www.bbc.co.uk /mundo /noticias /2013 /01/130114_rusia_ciberataque_octubre_rojo_men.shtml> [Consulted 10 April 2014]

[6] Garamore, J. (2012) "Panetta spells out DOD roles in cyberdefense" *American Forces Press Service.* 11 October 2012. Available at: <http://www.defense.gov /news/newsarticle.aspx?id=118187> [Consulted 22 May 2014]

advantages to it. However, this increasing openness is at the same time becoming a threat for all parties. As dependence on the Internet and information technologies grows, governments should invest proportionally in network security, incident response, technical literacy and international cooperation.

Moreover, this worrying reality is not limited to institutions; a huge number of private individuals have also suffered the attacks of viruses such as Zeus, Trojan horses, worms, botnets or logic bombs. The number of infected users has skyrocketed over the last years, which leads us to believe that, whichever the security measures taken by users according to their resources, nobody can ever be totally safe from these threats.

As we have seen, independently of whether one is a state or a private citizen, hackers, criminal organisations and other malicious entities can end up penetrating, disabling and destroying our information systems.

Due to all of the above, there is an urgent need for rewriting the rules of the game – that is, antivirus systems, early warning mechanisms and firewalls– in order to reduce the risk of suffering these attacks which, as we have seen, stop before no actor or international regulation.

3.2 Lack of consensus on the concept of 'use of force', forensic research and accountability

If we want to classify cyberattacks as a materialisation of the use of force, we first need to address the two following difficulties: firstly, the lack of consensus on what the 'use of force' actually is; and secondly, the problem arising when forensic post-cyberattack investigations are unable to clearly identify the culprit.

Regarding the first issue, until very recently the scope of the concept 'use of force' was explicitly limited to the use of armed force, as can be seen on the Charter of the United Nations. Here, the use of force is ostensibly limited to military measures, so that other interventions, however drastic or damaging, are not interpreted as 'use of force'[7].

If we analyse this situation from the current perspective on conflict resolution and the present concept of security, we will see that we are not prepared to react in an efficient and effective way to the damage caused by cyberattacks unless they are typified as an aggression. It is not reasonable to restrict the definition of 'use of force' to armed interventions; any channels liable to be used for aggression should be considered for it, including the malicious use of the Internet.

Reputable cybersecurity experts, such as Eugene Kaspersky, have said in numerous occasions that the cyberattacks of the latest years can reach the damaging potential of an 'atomic bomb'[8], even if in material consequences are not as visible.

Regarding the second concern, which is related to the difficulty in ascertaining who is responsible for cyberattacks, it is necessary to be cautious; when we qualify a digital operation as use of force, we are putting an action in the immaterial dimension on the same level as a material, physical armed aggression. We are comparing the consequences of an intangible action with those of a tangible one; therefore, forensic research processes become much more complex and, as a consequence, the assignation of responsibility cannot be carried out effectively or efficiently.

---

[7] United Nations. (1945) *United Nations Charter. Chapter VII, Art. 41, 24 October 1945*. Available at: <http://www.un.org/es/documents/charter/index.shtml> [Consulted 23 April 2014]

[8] Valenzuela, J. (2012) "Virus Flame: la primera bomba atómica de la ciberguerra" *El País*. [Online] 7 June 2012. Available at: <http://blogs.elpais.com/cronica-negra/2012/06/virus-flame-la-primera-bomba-atomica-de-la-ciberguerra.html> [Consulted 1 March 2015]

3.3 Vulnerabilities and solutions

The digital dimension, as we advanced in the first part, is nowadays characteristically anonymous, a fact which increases the already high vulnerability of states by preventing authorities from identifying those that are carrying out fraudulent actions with "sufficient capacity to cause a cyberattack with consequences similar to those due to the use of armed force, and to act diligently in accordance therewith"[9].

The development and metamorphosis of communication technologies has placed us at a point where traditional legal categories are revealing their weaknesses, especially as regards novel uses of force. Numerous cyberdefence and security actors and international organisations have asked for a doctrine on cyberwar defining clearly the rules for intervention required to deal with this threat. The absence of concrete rules, clearly only benefits those who are trying to violate other citizens' security and rights: "international law is tremendously underequipped to respond to situations such as the attribution of responsibilities for cyberattacks, causing these procedures to be carried out on political rather than scientific or legal criteria […] the disparate interests of nations in this area are threatening to cause a legal indefinition" [10].

This is yet another reason why we must search for the solution within Law and not at its margins, trying to work in the best possible way inside the limits within which International Law, for the time being, allows us to open new paths.

Conclusions

"Cyberspace is now a warzone where many of the decisive battles of the 21st century will be fought […] If they gain hold of a network, cyberwarriors can steal all the information it contains or instruct it to make money transfers, spill oil, free gas, derail trains or make aeroplanes crash" [11].

The reality of the present day is strikingly and characteristically complex. All the parts of the system are connected to one another through the Internet in a way such that the distinction between actions and consequences becomes blurred. We live in a permanently changing world where a global society has arisen, and where security is no more a fixed concept, its limits subject to constant redefinitions.

All these changes, and their effects on an international scenario, reveal that security, economic progress and human liberty are just as indissociable in the virtual space as they are in the physical space. Throughout this work, we have realised that the virtual space was never conceived with security or the need for protection in mind. After analysing its vulnerabilities we have managed to outline its main weaknesses – its Achilles' heels:

-The Internet lacks a system of governance. As it operates openly and unencrypted, it allows malicious traffic to exist and can do nothing to stop the propagation of cyberattacks.

-To respond to the new risks posed by cyberspace to the security and liberty of countries, institutions and citizens it is essential to strengthen international cooperation in information and communication technologies, as well as to improve early warning systems to avoid being the target of cyberwar, cyberespionage, cybercrime or cyberterrorism. As there is a dangerous strategic gap in this field, all countries without exception should begin promoting

[9] Torrecuadrada, S. (2013) "Internet y el uso de la fuerza". in *Ciberseguridad global. Oportunidades y compromisos en el uso del ciberespacio.* Ed. Universidad de Granada. Granada: Universidad de Granada, pp. 91-118.

[10] Gómez, A., "El ciberespacio como escenario de conflicto. Identificación de las amenazas" in *El ciberespacio. Nuevo escenario de confrontación.* Ed. Ministerio de Defensa. Madrid: Ministerio de Defensa, 2012, pp. 167-204.

[11] Clarke, R. and R. Knake, *Guerra en la red. Los nuevos campos de batalla.* Barcelona: Editorial Ariel, 2011.

collective actions for cyberattack prevention, something that has not been addressed effectively at the European level.

-In accordance with the former, the level of threat posed by cyberattacks, as we have had the opportunity to see, can hardly be exaggerated. Thus, the modernisation of cybersecurity systems, the fostering of a culture of cyberdefence and the promotion of cybersecurity research at all levels and dimensions are indispensable.

-Equally important, the development of cyberresilience is a task that cannot be delayed. We must aspire to being able to minimise the effects of cyberattacks and to recover operational capacity as quickly as possible. Thus, cybersecurity has to be understood as a long-term multidisciplinary task that can only be carried out through the collaboration and cooperation of all public and private agents. An integral, effective and efficient management of cyberspace must be achieved to deal coherently with menaces coming from within it.

-We must acknowledge that security in general and cybersecurity in particular are public matters and that, therefore, public-private cooperation is absolutely necessary to deal correctly and responsibly with cyberspace-based threats: "Nobody is free from risk, and therefore raising awareness of these risks is a mandatory and urgent need […] Public-private cooperation has been acknowledged by everybody as the only way of tackling this situation"[12].

Without further ado, I would like to conclude this international communication by reminding that effective and efficient responses to the security issues that arise from the 'cyberscape' can only be produced thanks to the work of dedicated institutions, such as the International Security Observatory or the Centre for Defence and Security Strategic Studies from the "Carol I" National Defence University.

Here, I would like to speak in support of research initiatives being carried out in universities throughout the world, both public and private; for I believe that they are the key tool for finding the solutions required for responding to the threats and challenges posed by cyberspace. It is from international forums, national cybersecurity strategies, universities and, specifically, European forums that the reflection on how to address the intrinsic issues of the 'cyberscape' has to be made.

Just as the violation of human rights can never be acceptable, Internet privacy and security should not become lost causes. We are witnessing the construction of a new landscape, a 'cyberscape', wherein cybersecurity holds the key to our future. It is our responsibility to guarantee that the Internet remains secure, for it is here that the interconnection and interdependence of us, the actors in the international system, is at its weakest.

BIBLIOGRAPHY:

1. Clarke, R. and R. Knake. (2011) *Guerra en la red. Los nuevos campos de batalla.* Barcelona: Editorial Ariel
2. Duva, J. (2014) "El 95% de los ciberdelitos cometidos quedan impunes" *El País.* [Online] 4 May 2014. Available at: <http://politica.elpais.com/politica/2014/05/03/actualidad/1399117342_ 852720.html#sumario_2> [Consulted 11 February 2015]

[12] Gómez, A., "El ciberespacio como escenario de conflicto. Identificación de las amenazas" in *El ciberespacio. Nuevo escenario de confrontación.* Ed. Ministerio de Defensa. Madrid: Ministerio de Defensa, 2012, pp. 167-204.

3. European Commission (2013) *The Cybersecurity Strategy Of The European Union An Open, Safe And Secure Cyberspace*. Brussels. [Online] Available at: <http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf> [Consulted 25 February 2015]
4. Garamore, J. (2012) "Panetta spells out DOD roles in cyberdefense" *American Forces Press Service.* 11 October 2012. Available at: <http://www.defense.gov /news/newsarticle.aspx?id=118187> [Consulted 13 February 2015]
5. Gómez, A. (2012) "El ciberespacio como escenario de conflicto. Identificación de las amenazas". in *El ciberespacio. Nuevo escenario de confrontación.* Ed. Ministerio de Defensa. Madrid: Ministerio de Defensa, pp. 167-204.
6. Kaspersky Lab. (2012) "Flame…The latest cyberattack. What are the risks -and is protection necessary for you?" in *Kaspersky Lab Corporate News* [Online] Available at: <http://www.kaspersky-sea.com/flame/> [Consulted 2 March 2015]
7. Lee, D. (2013) "Descubren en Rusia masivo ciberataque mundial". *BBC.* [Online] 15 January 2013. Available at: <http://www.bbc.co.uk /mundo /noticias /2013 /01/130114_rusia_ciberataque_octubre_rojo_men.shtml> [Consulted 10 January 2015]
8. López, J. (2012) "La evolución del conflicto hacia un nuevo escenario". in *El ciberespacio. Nuevo escenario de confrontación.* Ed. Ministerio de Defensa. Madrid: Ministerio de Defensa, pp. 117-166.
9. Naciones Unidas. (1945) *Carta de las Naciones Unidas. Capitulo VII, Art. 41. del 24 de octubre de 1945*. Available at: <http://www.un.org/es/documents/charter/index.shtml> [Consulted 23 April 2014]
10. Nakashima, E. (2013) "In cyberwarfare, rules of engagement still hard to define". *The Washington Post.* 10 March 2013. Available at: <http://www.washingtonpost. com/world/national-security/in-cyberwarfare-rules-of-engagement-still-hard-to-define/2013/03/10/0442507c-88da-11e2-9d71-f0feafdd1394_story.html> [Consulted 2 February 2015]
11. Torrecuadrada, S. (2013) "Internet y el uso de la fuerza". in *Ciberseguridad global. Oportunidades y compromisos en el uso del ciberespacio.* Ed. Universidad de Granada. Granada: Universidad de Granada, pp. 91-118.
12. Valenzuela, J. (2012) "Virus Flame: la primera bomba atómica de la ciberguerra" *El País.* [Online] 7 June 2012. Available at: <http://blogs.elpais.com/cronica-negra/2012/06/virus-flame-la-primera-bomba-atomica-de-la-ciberguerra.html> [Consulted 1 March 2015]

CYBER RISKS AND VULNERABILITIES, A CLEAR AND PRESENT DANGER

Emanoel MATEI
Faculty of Political Science, University of Bucharest, MA student, Bucharest, Romania,
e-mail: f117@astrospot.ro

Ioana Corina JULAN
Faculty of Political Science, University of Bucharest, student, Bucharest, Romania,
e-mail: julan.ioan-corina@fspub.unibuc.ro

Abstract: *The current paper is briefly exploring some of the main risks, threats and vulnerabilities in the cyberspace area. By extensively using various open sources we will analyze most important cyber attacks along the past year, such as the Sony attack towards the end of 2014 and explore the cyber vulnerabilities, risks and threats at national or lower levels and mobile security devices. We will try to categorize the exposure risks and will try to list, describe and briefly analyze the most important major vulnerabilities currently present in cyberspace. The paper is presented without pretence of completeness and is based on the extensive study of various open sources and of some important works in the field of Political Science, Strategic Studies and Cyberpower Studies.*

Keywords: *Cyber Attack, Cyber Risk, Cyber Vulnerability, Sony attack, Security Breach.*

This paper is not aiming at offering the readers a set of general facts about the whole area of cyber-threats. It's aiming a totally different goal by giving other perspectives on the 2014 cyber-threats cases. We will try at the beginning of this paper to explain the basic concepts use, in order to make easier for the reader to get a better understanding of the facts presented in the following sections.

Cyberspace is defined as being "a functional domain, defined by the use of electronics in order (...) to exploit information through interconnected systems and infrastructure associated with these"[1]. In addition to this definition present in a work of political science, there are more technical definitions that define cyberspace as "a global domain within the information environment consisting of the interdependent network IT infrastructure and ICT, including the Internet, telecommunication networks, computer systems and embedded processors and controllers."[2]

For Daniel Kuehl, Professor of Systems Management at the Information Operations and Assurance Department, Information Resources Management College, of the National Defense University at Ft. McNair, Virginia, cyberspace is "an operational domain framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interconnected and Internetted information systems and their associated infrastructures."[3]

---

[1] Robert O. KEOHANE and Joseph S. NYE, "Power and Interdependence: World Politics in Transition", Little Brown, Boston, 1977, p. 131

[2]U.S. Department of Energy, "Electricity Subsector Cybersecurity", p.67, accessed on March 25, 2015 at the Internet address http://energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20%20 Final%20-%20May%202012.pdf

[3] Department of Defense, "2006 Quadrennial Defense Review Report", Washington, DC: Department of Defense, February 6, 2006, accessed on March 25, 2015 at the Internet address

Cyber-attacks – hacking of various kinds – are a fact of modern life. Over time there have been a multitude of state actors accused of taking part in cyber-attacks directed against other states, companies or citizens with various jobs and responsibilities. There are also individuals or groups of well-trained individuals who jointly operate, in order to get access to various non-public pieces of information which they are later using in one form or another. Thousands of detected intrusions occur each day, but there are some that remain undetected for a long period of time, going on with recording information, giving the attackers continuous access to the compromised system or network. There are concerns that the attacks may be used for geo-strategic purposes in order to collect sensitive information, test the security strength of the targeted state and the reaction capability to deter such attacks.

Cyberpower – represent the ability to use a well-defined number of cyberspace resources to create advantages and leverage in all the other operational environments combined with instruments of power.[4]

Cyber threats – this kind of threats has a tremendous impact on our daily life, businesses or some essential social institutions and services. The most recent example of cyber-threat happened at the launch of the Sony Pictures movie "The Interview" when the attackers got access to names, address, social security numbers and other financial information of a large number of employees, threatening them with further physical actions, both against them and their family members.

Cyber Terrorism – is the convergence of terrorism and virtual space, with attacks against computers and networks, to intimidate a government or a nation.

The *Cyber* concept refers to a place where data can be exchanged between various interconnected systems, routers and other electronic devices using the same protocol of communication and obeying to the same network rules. Nowadays, this is one of the most important and easiest ways to reach influence, a way available for any entity, large or small, public or private: companies, organizations, individuals, terrorists. It deserve a further discussion of whether the cyberspace is a domain comparable to other "regular domains" such as land, sea, air and space analyzed in traditional geopolitical contexts.[5]

Hacking in general designates operations which exploit computers or bypass security systems with the help of specially crafted (and malicious) software.

Hackers are individuals with high technical knowledge, spending endless hours honing their skills. Most of them are driven by curiosity and challenging themselves to see if they can disrupt the computer system. We should not consider curiosity in this case a terrorist act. But such abilities can be used in terrorist activities, too.

We have to understand that our world, if we like it or not, is becoming more and more interconnected. Cyberspace is expanding from our usual computers to more and more usual domestic items: microwave ovens, refrigerators, air conditioners, TV sets, giving us a better place to live in, and a better control over our own comfort and lifestyle. *Cyberspace is becoming more 'real' as we inevitably become more 'virtual'. The old military notion of a continuous and easily recognizable front line becomes outdated with each passing day, and all of us are now in the 'front line' of the battle. To win the battle we need to develop a set of cyber tools and a positive attitude of large population groups. But it is very clear that these different types of attacks that take place in cyberspace can influence the outcome of major events taking place on the international scene.*

---

http://www.defense.gov/qdr/report/Report20060203.pdf

[4] *Ibidem.*

[5] *Ibidem.*

1. The ISIL case - Cyber Terrorism *on* Social Media

Islamic State of Iraq and the Levant (ISIL) was the first organization which massively and really systematically uses social media to spread fear. Their movies cause uproar at global level, making ISIL better known than any other previous terrorist organization or structure. Using *Twitter, Facebook, Liveleak, YouTube* and other well-known websites they have targeted a massive number of people to spread rumors about their own existence and publicly shared agenda. ISIL has applied the same advertising vectors as any Western business company does. Our society regularly absorbs a lot of breaking news, and social media networks are the perfect soil for such news propagation. Strangely, their targets are converted in transmitters when the information hits them. Even if the motivation is a completely different one, with each individual who spreads the news further, the message is becoming even louder and is capturing an unexpectedly large audience. The propaganda goal is accomplished. Such a pattern was reported by *Time.com* on September 11, 2014: "terrorists love Twitter. That includes the Islamic State of Iraq and the Levant (ISIL), the Sunni Muslim extremists whom the U.S. is targeting in an expanded military campaign. ISIL has emerged as the most sophisticated group yet at using the service to spread its bloodthirsty message."[6]

We cannot have any immediate countermeasures to suppress the message, but in the long run, these messages can affect the morale of large populations. Social media users are, in many occasions, eager to see any kind of counter-action from the authorities, so that the anti-propaganda movies or even a military strike against their terrorist organization is many times welcomed.

The other problem is recruitment. This type of propaganda can make a large number of people willing to start a dangerous adventure for a virtual cause. The number of "volunteers" is growing and websites are a powerful tool for extremist organizations of all sorts. According to an open source "in recent years, online recruiters have successfully won over Westerners, including Americans"[7], said Rita Katz, the Director and co-founder of the SITE Intelligence Group[8], who has studied, tracked, and analyzed international terrorists, the global jihadist network and terrorism financing for more than a decade.

Terrorist organizations can go easily to the next level anytime - crowdfunding or social funding and start gathering money from even more supporters. They can use various types of e-coins to get the actual money in their pockets, directly from the donors. This can mobilize supporters to play an active role and support the cause. On January 29, 2015 an open source reported that "a Tel Aviv analyst working for a Singapore-based cyber intelligence company says he has uncovered concrete evidence that a terror cell, purporting to be related to Islamic State and operating in the Americas, is soliciting for Bitcoins as part of its fundraising efforts."[9]

The internet is a safe haven for terrorists. They don't need to travel and are fully able to stay anonymous. Terrorists can also hide their messages using the internet as a 'transportation device' for their encrypted communication channel.

---

[6] Alex ALTMAN, "Why Terrorists Love Twitter", Time, September 13, 2014, accessed on March 25, 2015 at the Internet address http://time.com/3319278/isis-isil-twitter/?xid=newsletter-brief

[7] Maria VULTAGGIO, "ISIS Online Recruitment: 3 Colorado Teenage Girls A Textbook Case", Ibi Times, November 11, 2014, accessed on March 25, 2015 at the Internet address http://www.ibtimes.com/isis-online-recruitment-3-colorado-teenage-girls-textbook-case-1722155

[8] SITE Intelligence Group is a for-profit Bethesda, Maryland-based company that tracks online activity of White supremacist and Jihadi organizations.

[9] Donna HARMAN, "U.S.-based ISIS cell fundraising on the dark web, new evidence suggests", *Haaretz*, January 29, 2015, accessed on March 25, 2015 at the Internet address http://www.haaretz.com/news/middle-east/.premium-1.639542

2. Sony Attack towards the end of 2014

At the end of 2014 *Sony Pictures* was hit by a major attack. In this particular case we can certainly say that the attack had multiple vectors. It's an example that evokes the significant differences between the power of state actor and the power capabilities of a large company.

The attack was, as far as we know, based on a zero day vulnerability (a vulnerability discovered after using the same operating system or service by someone looking for these types of security holes), and mapping the entire *Sony Pictures* network until the internal topology of their network was exposed to the attacker. On the second phase of attack, the hackers started to extract data from the network, including company internal emails, personal and financial data of the employees.

An unknown group called themselves *Guardians of Peace* claimed it was behind the attack. The perpetrators were North Korean hackers and on that particular night they have worked, as far as we know, from a hotel in Thailand.[10]

This attack forced *Sony* to postpone the movie premiere and *Sony* public image suffered a lot. *Sony* actually bought time to evaluate the entire network and check every system and intrusion path. With the help of NSA and FBI, *Sony* was able to identify the intrusion path and other relevant information linking North Korea to the attack. Employees were forced to leave their electronics and do their work using pen, paper, and fax machines after the hack.

Hackers also stole five *Sony* movies unreleased by that date, and made them public on the file-sharing networks, causing a huge financial loss to the company. They have also exposed many private email conversations of the top management.

It's hard to avoid such attacks and make a 'bulletproof' network. North Korea developed its cyber operations for obvious reasons, a system called "Red Star OS".

Sony's lack of internal security led to this massive public data disclosure. The missing internal security layers and levels, combined with not having an intrusion detection system (a computer or piece of software that can monitor suspicious activity, policy violation and report to the management or computer technicians) made everything possible.

3. Attacks against NATO

As we've stated before, hackers usually take advantage of computers by using undiscovered bugs. On October 2014, Russian hackers has exploited a bug found (and not reported) in Microsoft Windows to spy the computers of several NATO structures, of the European Union, and computers in Ukraine and in companies active in the telecom and energy fields.[11] *The attacks were totally different from any other presented so far*. The perpetrators used, among others, a technique called "Social Engineering", when users received an email which seems to come from legitimate source, were lured to start the piece of software attached to the email and the hackers gained access to the affected system. Usually these types of attacks silently disable the computer protection including operating system firewall and virus protection.

---

[10] Cheryl K. CHUMLEY, "Guardians of Peace hackers thank Sony for scrubbing 'The Interview'", *Washington Times*, December 19, 2014, accessed on March 25, 2015 at the Internet address http://www.washingtontimes.com/news/2014/dec/19/guardians-of-peace-hackers-thank-sony-for-scrubbin/

[11] Jim FINKLE, "Russian hackers target NATO, Ukraine and others: iSight", *Reuters*, October 14, 2014, accessed on March 25, 2015 at the Internet address http://www.reuters.com/article/2014/10/14/us-russia-hackers-idUSKCN0I308F20141014

Looking at the information they can get from the affected systems we can conclude the hackers were state-sponsored or hired as contractors, but it's hard to pinpoint the exact state even if we can speculate.

A serious recent study including policy recommendations is stating that "cyber-attacks can range from small attacks that cause minor damage to very large attacks that can inflict massive damage. It is hard to point to any specific threshold of potential cyber damage below which U.S. strategy should discount an attack, but above which an attack should trigger concern for deterrence, coupled with the possibility of retaliatory response. The ladder of escalation contains many rungs of ascending provocation and damage, each of which could merit a response, of increasing intensity. A U.S. cyber deterrence strategy might be shaped to identify decisive, proportional responses at each rung of the ladder, rather than trying to specify a single threshold that separates nonresponses from strong responses."[12]

Responding to an attempt to break the protection of NATO computer systems or disruption of electronic communication, must be analyzed and properly sized. If the attack has a lower impact and amplitude the attacker can be stopped using conventional means like firewall or IDS systems. On a large scale or a coordinated attack, threat can be filtered out directly from the continental internet backbones.

4. New Challenges of the dynamic cyber zone

"Reflecting how all international conflicts now have some digital component, NATO has updated its cyber defense policy to make it clear that a cyber-attack can be treated as the equivalent of an attack with conventional weapons"[13], open sources report.

On September 5, 2014, Sorin Ducaru, NATO's Assistant Secretary General for Emerging Security Challenges, stated that "Article V of the Treaty is extended for disinformation, subversion and cyber-attacks."[14] The clause states an attack against one member of NATO "shall be considered an attack against them all"[15].

According to a reliable open source, Jamie Shea, the official in charge of emerging security threats, said that "recognizing cyberspace sabotage as an act of war is only halfway to a coherent policy" and added that "we don't say exactly which circumstances or what the threshold of the attack has to be to trigger a collective NATO response and we don't say what the collective NATO response should be." But an attitude of "'we'll know it when we see it,' is not a strategy." In the same article, James G. Stavridis, the dean of the Fletcher School of Law and Diplomacy at Tufts and the former NATO Supreme Allied Commander and Dave Weinstein (a former strategic planner at US Cyber Command) underlined two major problems: that the effects of "cyber attacks that threaten loss of life or cause physical damage to infrastructure" must "be considered cumulatively over time and not just case by case", and secondly choosing the exact moment when Article 5 must be invoked, because according to

[12] Franklin D. KRAMER, "Cyberpower and National Security: Policy Recommendations for a Strategic Framework", March 2014, accessed on March 25, 2015 at the Internet address http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-01.pdf

[13] Steve RANGER, "NATO updates cyber defence policy as digital attacks become a standard part of conflict", *ZDNet*, June 30, 2014, accessed on March 25, 2015 at the Internet address http://www.zdnet.com/article/nato-updates-cyber-defence-policy-as-digital-attacks-become-a-standard-part-of-conflict/

[14] Ioana Corina JULAN, "News Alert No.15: NATO Summit in Wales: CyberAttacks, integrated in Article V", *Morgenthau Center*, September 5, 2014, accessed on March 25, 2015 at the Internet address http://morgenthaucenter.org/news-alert-no-15-nato-summit-in-wales-cyberattacks-integrated-in-article-v/

[15] "The North Atlantic Treaty" at the Internet address http://www.nato.int/cps/en/natolive/official_texts_17120.htm

them there is a important number of various cyber-attacks "that are physically harmless but cause severe economic damage".[16]

Modern technology allows social relations across huge spaces. The borders don't matter anymore. People from a "remote area" can interact and influence people from other areas. As transformation in communication is accelerated and cheaper, we need to reshape the patterns of social control including collecting and data interpretation. The need to counter the potential risk of the widespread damage generated by a large scale cyber-terrorist attack forces the authorities to design and implement strategies aimed at developing narrow but very precise pre-emptive secret intelligence and new cooperative measures. Through its Cyber Defence Management Authority (CDMA), NATO has the authority to respond quickly to cyber-attacks on its members and deploy support teams, but this type of intervention can be filtered down to national levels in the future.

According to the NATO official webpage, "against the background of increasing dependence on technology and on the Internet, the Alliance is advancing its efforts to confront the wide range of cyber threats targeting NATO's networks on a daily basis. The growing sophistication of cyber attacks makes the protection of the Alliance's communications and information systems (CIS) an urgent task. This objective has been recognised as a priority in NATO's Strategic Concept, and has been reiterated in the two most recent Summit Declarations, as well as at NATO ministerial meetings."[17]

Another problem is the one of cyber espionage, mostly the campaigns of state-sponsored hacking. Last year in November, a report published by *Kaspersky*, a software security group with more than 300 million users and 250,000 corporate clients worldwide in almost 200 countries, analyzed in a detailed way a new type of cyber attack that can easily be considered espionage. "For the past seven years, a strong threat actor named Darkhotel, also known as Tapaoux, has carried out a number of successful attacks against a wide range of victims from around the world. It employs methods and techniques which go well beyond typical cyber-criminal behavior.[..] The targeting of top executives from various large companies around the world during their stay at certain 'Dark Hotels' is one of the most interesting aspects of this operation", the report is stating.[18] "As we have stated in an brief article published at that time, "due to the nature of the attacks - exact targeting - the episodes we are speaking about might be an indicator of a powerful political actor with global interests."[19]

As an example in the distribution of targets in December 2014 at the top of the list are industry, government and education. (Figure no.1)

---

[16] James G. STAVRIDIS and Dave WEINSTEIN, "NATO needs strong policy against cyber threats", *Boston Globe*, August 22, 2014, accessed on March 25, 2015 at the Internet address http://www.bostonglobe.com/opinion/2014/08/22/nato-needs-strong-policy-against-cyber-threats/cetoHkprGGZHMUAjfOhjHJ/story.html

[17] "Defending against cyber attacks", *North Atlantic Treaty Organization*, October 9, 2012, at the Internet address http://www.nato.int/cps/en/natohq/75747.htm

[18] "The DarkHotel Apt - A Story of Unusual Hospitality", *Kaspersky*, November 2014, accessed on March 25, 2015 at the Internet address https://securelist.com/files/2014/11/darkhotel_kl_07.11.pdf

[19] Ioana Corina JULAN, "News Alert No.90: A cyber-threat with precise targets", *Morgenthau Center*, November 14, 2014 at the Internet address http://morgenthaucenter.org/news-alert-no-90-a-cyber-threat-with-precise-targets/

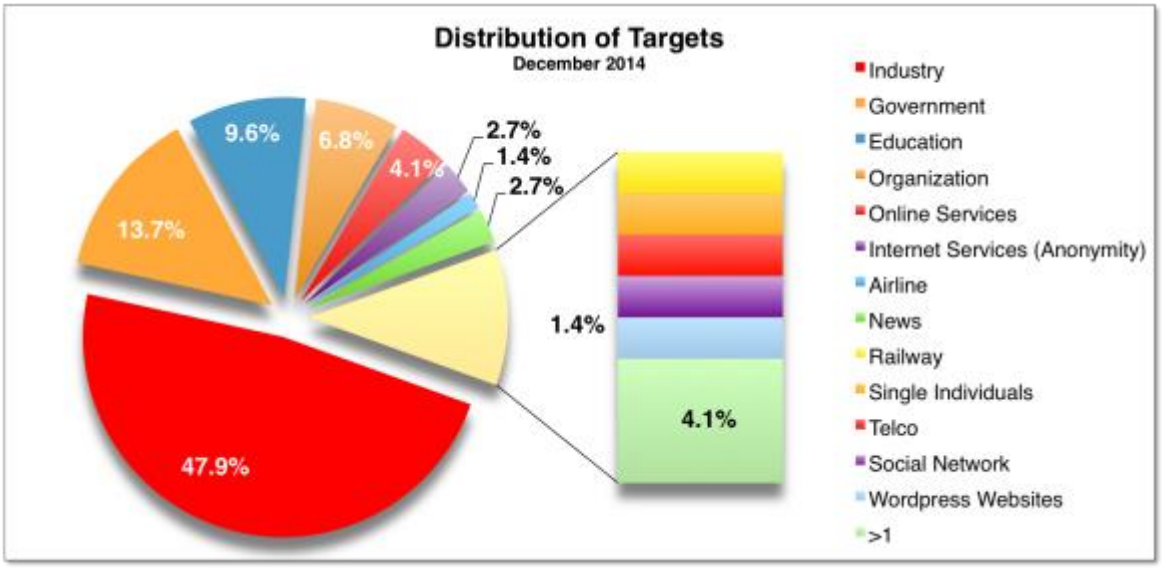


Figure no.1
Distribution of Targets in December 2014[20]

As the threats are more and more visible, the cyber world is reshaping itself picturing a mirror for the physical and tangible realities. Recognizing cyberspace sabotage against NATO, already ongoing cyber alliances between Russia and China[21], the large investments in cyber security in Israel[22], boosting cyber spending twelve times (a 1,200 % increase!) by Iran[23] and many other examples are very clear signs of the major and increasing importance of this new area – cyber defense aimed at deterring, stopping and 'defeating' cyber threats and cyber attacks – for both the present and the future of national security in most states. The need for clarity and policies in the area is more and more urgent, and as DTCC[24] stated in the 2014 report, quite clearly sharply increased "further action at both the national and international levels of government legislation and regulation to address cyber threats is needed".[25]

BIBLIOGRAPHY:

1. AWAN, Imran and BLAKEMORE, Brian, "Policing Cyber Hate, Cyber Threats and Cyber Terrorism", Ashgate Publishing, 2012

[20]"December 2014 Cyber Attacks Statistics", *Open Sources Info* accessed on March 25, 2015 at the Internet address http://opensourcesinfo.org/december-2014-cyber-attacks-statistics/
[21] Ioana Corina JULAN, "News Alert No.72: A potentially dangerous cyber-alliance: China and Russia", *Morgentahu Center*, October 22, 2014, accessed on March 25, 2015 at the Internet address http://morgenthaucenter.org/news-alert-no-72-a-potentially-dangerous-cyber-alliance-china-and-russia/
[22] Jason HINER, "How Israel is rewriting the future of cybersecurity and creating the next Silicon Valley", *Tech Republic*, accessed at March 28, 2014 at the Internet address http://www.techrepublic.com/article/how-israel-is-rewriting-the-future-of-cybersecurity-and-creating-the-next-silicon-valley/
[23] Cory BENNETT, "Iran has boosted cyber spending twelvefold", *The Hill*, March 23, 2015 at the Internet address http://thehill.com/policy/cybersecurity/236627-iranian-leader-has-boosted-cyber-spending-12-fold
[24] According to their website (http://www.dtcc.com/), "with over 40 years of experience, DTCC is the premier post-trade market infrastructure for the global fiancial services industry", accessed on March 25, 2015 at the Internet address
[25] Mark CLANCY and Michael LEIBROCK, "Cyber Risk – A Global Systemic Threat", October 2014, accessed on March 25, 2015 at the Internet address http://www.dtcc.com/

2. CARR, Jeffrey, “Inside Cyber Warfare: Mapping the Cyber Underworld”, O'Reilly Media, 2009
3. CLANCY Mark and LEIBROCK Michael, “Cyber Risk – A Global Systemic Threat”, October 2014 at the Internet address http://www.dtcc.com/
4. CLARKE, Richard A., “Cyber War”, Harper Collins e-books, 2010
5. Department of Defense, “2006 Quadrennial Defense Review Report”, Washington, DC: Department of Defense, February 6, 2006, accessed on March 25, 2015 at the Internet address http://www.defense.gov/qdr/report/Report20060203.pdf
6. http://energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf
7. KEOHANE, Robert O. and NYE, Joseph S., “Power and Interdependence: World Politics in Transition”, Little Brown, Boston, 1977
8. KRAMER, Franklin D., STARR H., WENTZ, Larry, “Cyberpower and National Security”, National Defense University, Potomac Books Inc., 2009
9. STAVRIDIS, James G. and WEINSTEIN, Dave, “NATO needs strong policy against cyber threats”, Boston Globe, August 22, 2014, accessed on March 25, 2015 at the Internet address http://www.bostonglobe.com/opinion/2014/08/22/nato-needs-strong-policy-against-cyber-threats/cetoHkprGGZHMUAjfOhjHJ/story.html
10. The DarkHotel Apt - A Story of Unusual Hospitality”, Kaspersky, November 2014, at the Internet address https://securelist.com/files/2014/11/darkhotel_kl_07.11.pdf
11. U.S. Department of Energy, “Electricity Subsector Cybersecurity”, accessed on March 25, 2015 at the Internet address

CORRELATED ANALYSIS OF PHYSICAL PROTECTION AND CYBER SECURITY MEASURES FOR NUCLEAR SITES

Tudor RADULESCU
PhD Student, "CAROL I" National Defence University, Bucharest, Romania,
e-mail: t.radulescu@gmail.com

***Abstract**: Physical protection systems for nuclear sites are designed, in most cases, based on a Design Basis Threat, following a quantitative approach. Evaluation of physical protection measures can make use of number and capabilities of attackers, detection probability, false alarm rate, and susceptibility to environmental factors for sensors and delay times for physical barriers.*

Information systems used in nuclear sites (DCS/SCADA, business network, classified information systems and physical protection digital systems) are designed for functionality rather than for intrinsic security, the cyber security measures and systems being implemented as add-ons. Cyber design basis threat is often defined in general terms and it cannot quantify the credible attack, as the capabilities of cyber criminals evolve faster than the DBT updates can follow.

In this paper we look at the different approaches for analysing physical protection and cyber security measures, evaluating the similarities and underlining the need for a correlated cyber-physical security analysis.

***Keywords**: security analysis, physical security, cyber security, nuclear, design basis threat*

Introduction

Since more than 40 years ago, specialists in the military, intelligence, law enforcement and private security engineering companies have contributed to setting up a well regulated environment for the design, operation and evaluation of the physical protection systems. The first major international guide on physical protection of nuclear sites has been published by the International Atomic Energy Agency (IAEA) in 1972, under the title "Recommendations for the Physical Protection of Nuclear Material", which has been dubbed "INFCIRC/225" in 1975.

Romanian CNCAN published its "Norm for Physical Protection in Nuclear Field (NPF-01)"[1] in 2001.

Cyber security concerns in the nuclear industry gain momentum much later. The first widely mediatized cyber security event took place at the Davis Besse Nuclear Power Plant, in 2003, when the Slammer worm infected process computers of the plant, following which "the plant's Safety Parameter Display System and Plant Process Computer were disabled for several hours"[2].

[1] "*Normele de Protecţie fizică în Domeniul Nuclear*", accessed 14.03.2015, on http://www.cncan.ro/assets/NPF/npf01.pdf

[2] Miller, Bill, Dale Rowe, "*A survey of SCADA and critical infrastructure incidents*", Proceedings of the 1st Annual conference on Research in information technology, ACM, 2012, p. 53

Cyber security regulations for the nuclear sector have appeared later, with NRC publishing its first guide in 2009, as Title 10, Code of Federal Regulations, Part 73, "Protection of digital computer and communication systems and networks"[3].

There is a maturity gap between the two fields, physical protection and cyber security, which reflects on the way the fields are regulated and on how the measures are evaluated.

1. Physical Protection Systems Evaluation

The design of physical protection measures for nuclear sites is based, in most cases, on a design basis threat (DBT) that quantifies the characteristics of the attacker.

According to the "Development, Use and Maintenance of the Design Basis Threat" guide published by the IAEA, "DBT is the State's description of a representative set of attributes and characteristics of adversaries, based upon (but not necessarily limited to) a threat assessment, which the State has decided to use as a basis for the design and evaluation of a physical protection system."[4]

This approach allows specialists to predict, control and quantify the performance of the physical protection systems.

The DBT concept has been introduced in 1979 by the US NRC (Nuclear Regulatory Commission). In Title 10, Code of Federal Regulations, Part 73, there is a standard description of a design basis threat, which covers: "A determined violent external assault [...] and [...] An internal threat; and [...] A land vehicle bomb assault [...] and [...] waterborne vehicle bomb assault [...] and [...] A cyber attack"[5].

The public descriptions of the DBT are provided for reference only, while the quantitative description of the DBT is classified. An example of a detailed description is available in the course material provided at the IAEA DBT Workshops: "Attempt of theft of a significant amount of NM (e.g. 10Kg of Pu) by a group of 6 outsiders equipped with 10 Kg TNT explosive, automatic weapons (including light infantry weapons) and specific commercially available intrusion tools. They have a comprehensive knowledge of the facility and associated PP measures. Willing to die or to kill. No collusion with insider."[6]

Based on such quantitative information, the physical protection measures can be designed in such a way that:

- the protected targets (vital areas) comprise any location that hosts nuclear materials (plutonium) in significant quantities;
- the intrusion detection systems are suitable to detect military trained intruders, with high mobility / equipped with light baggage (few kg of explosives and infantry weapons), with comprehensive knowledge of the facility, of the vulnerabilities of the detection systems and physical barriers and with tools to sabotage an intrusion detection system;
- the physical barriers on any possible adversaries paths can withstand attacks with explosives with cumulative quantities of 10 Kg;

[3] "*Title 10, Code of Federal Regulations, Part 73.54, Protection of digital computer and communication systems and networks*", accessed 15.03.2015, on http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html

[4] "*Development, Use and Maintenance of the Design Basis Threat*", accessed 15.03.2015, on http://www-pub.iaea.org/MTCD/publications/PDF/Pub1386_web.pdf, p. 8.

[5] "*Title 10, Code of Federal Regulations, Part 73.1*", accessed 15.03.2015, on http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0001.html

[6] "*Design Basis Threat (DBT) Workshop, Session 7, What Could a DBT Look Like?*", DBT Workshop, IAEA, Bucharest, Romania, 2012.

- the physical barriers offer significant delay to commercially available intrusion tools, in such a way that the delay is more than the time required by the reaction force to intercept the attackers;
- the reaction force is sized in such a way that they have a neutralization probability higher than 90% against a team of 6 attackers armed with lights infantry weapons and with the willing to have up to 5 members killed in order to attain the mission goal.
- There are critics against the DBT approach, stating that it "does not attempt to account for the strategic nature of terrorists, except regarding their valuation of various targets"[7]. The cited article proposes three alternatives to the DBT approach:
- Tiered threat levels – an alternative which specifies three levels of DBT; we do not consider this approach as different from the classic DBT approach for evaluating the performance of security measures;
- Security Culture – it is merely a complementary tool to the DBT and does not add elements that contribute to the evaluation;
- Game Theory – an approach based on the idea that "a terrorist's expected payoff from an attack is actually a function of three factors: the probability that the specific attack will succeed, the consequences if that attack is successful, and the value of those consequences to the terrorist"[8]. This approach combines the elements included in the process of Vital Area Identification ("Accessibility, Standoff Attack, Detectability, Target Attractiveness"[9]) with elements of probability of attack success, which is the inverse of the probability of neutralization, for which "no acceptable standardized methodology exists"[10].

The design for physical protection takes into account basic principles of "Defence in depth, minimum consequence of component failure, balanced protection and Graded protection in accordance with the significance or potential radiological consequences."[11] The main aspects considered during the design are detection, delay, response and measures for deterrence and mitigation of insider participation.

Physical protection sensors can be characterized in terms of detection probability, false alarm rate, and susceptibility to environmental factors adverse effects, while physical barriers can be characterized in terms of delay, based on the capabilities of the adversary tools. The designer can precisely prescribe the detection and delay layers in order to allow the reaction force to interrupt and neutralize the adversary.

The evaluation of a physical protection system starts with an analysis of the design and a site walk-down to assess the actual implementation of the system. Based on the design documentation, the site model can be developed. The most common method for measures effectiveness analysis is the use of the Pathway Analysis. The analysis "involves identifying

---

[7] Kuperman, Alan J., Kirkham, Lara, "*Protecting U.S. Nuclear Facilities from Terrorist Attack: Re-assessing the Current "Design Basis Threat" Approach*", prepared for INMM 54th Annual Meeting, Palm Desert, CA, 2013, accessed 15.03.2015, on http://sites.utexas.edu/nppp/files/2013/07/INMM-2013-July-paper.pdf, p. 5.

[8] Kuperman, Alan J., Kirkham, Lara, "*Protecting U.S. Nuclear Facilities from Terrorist Attack: Re-assessing the Current "Design Basis Threat" Approach*", prepared for INMM 54th Annual Meeting, Palm Desert, CA, 2013, accessed 15.03.2015, on http://sites.utexas.edu/nppp/files/2013/07/INMM-2013-July-paper.pdf, p. 6.

[9] Malachova, Tereza, Malach, Jindrich, Vintr, Zdenek, "*Threat characterization in vital area identification process*", Proceedings of the 47th International Carnahan Conference on Security Technology (ICCST), vol., no., pp.1,6, 2013

[10] Whitehead, Donnie, Potter, Claude, O'Connor, Sharon, "*Nuclear Power Plant Security Assessment Technical Manual*", Sandia Report SAND2007-5591, 2007, accessed 15.03.2015, on http://prod.sandia.gov/techlib/access-control.cgi/2007/075591.pdf, p. 39.

[11] "*Guidance and considerations for the implementation of INFCIRC/225/Rev.4, The Physical Protection of Nuclear Material and Nuclear Facilities,IAEA-TECDOC-967 (Rev.1)*", IAEA, 2000, accessed 15.02.2015, on http://www-pub.iaea.org/MTCD/publications/PDF/te_967rev1_prn.pdf, p. 4.

and analysing the paths (through a facility) that an adversary might take during his theft or sabotage attempt [...]. An adversary path is an ordered series of actions against a target that, if completed, results in successful theft or sabotage."[12]

Using this approach, the site is modelled by determining, for each vital area, the complete set of credible adversary paths, consisting of areas, actions, detection elements and physical barrier elements, resulting in the adversary sequence diagram - ASD (see Figure no. 1).

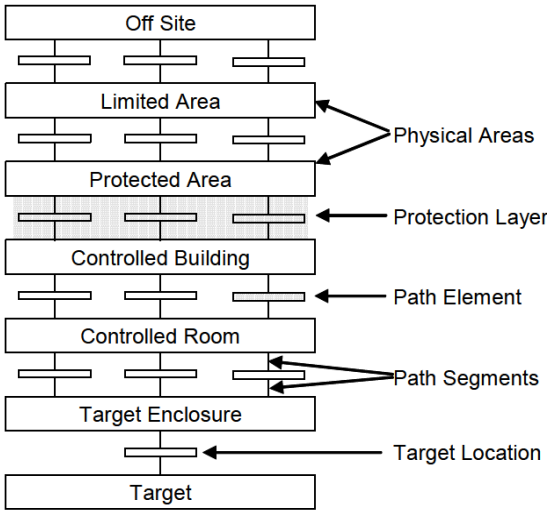


Figure no. 1 Basic adversary sequence diagram[13]

Each element is characterized with specific properties:

- dimensions (to account for the delay of traversing areas)
- physical barrier characteristics (to provide information on the delay time based on the tools available with the attackers – mechanical and electrical tools, explosives)
- detection elements with associated probabilities and complementary technology advantage (providing immunity to stealth attack tactics)
- human element (as detection factor and, if armed, delay factor)

Based on the ASD, it is possible to assess the Critical Detection Point (CDP) and the Probability of Interruption (P_I). CDP is the last point across the adversary path where the detection elements still matter, which means the reaction force still has enough time to interrupt the intrusion. Any detection element after this point is useless for the purpose of the physical protection system. P_I is the cumulative probability that the attackers are detected up to the CDP. The path with the lowest P_I is called Critical Path.

The modelling of the facility and the subsequent calculations can be performed with specialized computer software tools, such as EASI (Estimate of Adversary Sequence Interruption)[14], SAVI (Systematic Analysis of Vulnerability to Intrusion)[15], Analytic System

[12] Whitehead, Donnie, Potter, Claude, O'Connor, Sharon, "*Nuclear Power Plant Security Assessment Technical Manual*", Sandia Report SAND2007-5591, 2007, accessed 15.03.2015, on http://prod.sandia.gov/techlib/access-control.cgi/2007/075591.pdf, p. 31.

[13] Whitehead, Donnie, Potter, Claude, O'Connor, Sharon, "*Nuclear Power Plant Security Assessment Technical Manual*", Sandia Report SAND2007-5591, 2007, accessed 15.03.2015, on http://prod.sandia.gov/techlib/access-control.cgi/2007/075591.pdf, p. 37.

[14] Garcia, Mary Lynn, "*The Design and Evaluation of Physical Protection Systems*", 2nd ed. Burlington, MA, Elsevier Butterworth–Heinemann, 2008

[15] "*SAVI: Systematic Analysis of vulnerability to Intrusion*", Volume 1 of 2, SAND89-0926/1 Sandia National Laboratories, Albuquerque, New Mexico, 1989.

and Software for Evaluating Safeguards and Security (ASSESS)[16] and Systematic Analysis of Physical Protection Effectiveness (SAPE)[17].

The data used in the numeric simulations can be extracted from databases generated in laboratory tests (some of the tools enumerated above already have generic performance data included in the software package), or can be determined by tests of similar elements in laboratories.

The next stage of the evaluation is the determination of the Probability of Neutralization (P_N). P_N is determined using software models based on Markov Chains. The probability is determined based on number of attackers and their fire power, and subsequent layers of defenders, characterized by numbers and fire power.

More complex P_N calculations can be determined with armed conflict simulation tools (war games) as JCATS (Joint Conflict and Tactical Simulation). The JCATS program "typically simulates a battle between two opposing sides (often called red and blue forces), but it can accommodate up to 10 sides with friendly, enemy, and neutral relationships"[18].

Physical protection measures analysis comes down to calculating the probability of system effectiveness P_E, which is: $P_E = P_I * P_N$.

Apart from the theoretical numerical simulations, based on the actual design, results are validated using scenario analyses, table-top exercises and force on force exercises.

2. Cyber Security Systems Evaluation

Cyber systems in nuclear sites have been implemented since before the term cyber security has been used. The first use of the "cyber security" term is not referenced in the consulted bibliography, but it is generally linked with the coining of the term "cyberspace" by William Gibson, in a short story published in 1982[19], then in the novel "Neuromancer" in 1984.

The first regulation regarding cyber security for nuclear installations has been published in 2009, when NRC published Title 10, Code of Federal Regulations, Part 73, "Protection of digital computer and communication systems and networks"[20]. It sets the general responsibilities and has no technical guidance for implementation.

In the "Norm regarding the protection of nuclear installations against cyber threats" published by CNCAN, the same approach of defining roles and responsibilities is used. However, the document sets the categories of systems, components and equipment (SCE) to be protected against cyber threats: "SCE with functions of nuclear security; SCE that are part of the physical protection system; SCE which are part of the nuclear material accountability

[16] Al-Ayat, R.A., Cousins, T.D., Hoover, E.R., "*ASSESS (Analytic System and Software for Evaluating Safeguards and Security) update: Current status and future developments*", Institute of nuclear materials management conference, Los Angeles, CA (USA), 1990.

[17] Jang, Sung Soon, Kwak, Sung-Woo, Yoo, Hosik, Kim, Jung-Soo, Yoon, Wan Ki, "*Development of a Vulnerability Assessment Code for a Physical Protection System: Systematic Analysis of Physical Protection Effectiveness (SAPE)*", Nuclear Engineering and Technology, Vol. 41 No.5, 2009, accessed 15.03.2015, on http://www.kns.org/jknsfile/v41/JK0410747.pdf

[18] Heller, Arnie, "*Simulating Warfare Is No Video Game*", Science & Technology Review, Lawrence Livermore National Laboratory, January/February 2000, accessed 15.03.2015, on https://str.llnl.gov/str/pdfs/01_00.1.pdf

[19] Gilles, Martin, "*Defending the digital frontier*", The Economist, 12 July 2014, accessed 15.03.2015, on http://www.economist.com/news/special-report/21606416-companies-markets-and-countries-are-increasingly-under-attack-cyber-criminals

[20] "*Title 10, Code of Federal Regulations, Part 73.54, Protection of digital computer and communication systems and networks*", accessed 15.03.2015, on http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html

system (nuclear safeguards); SCE with functions in emergency response, including communication systems used in emergency situations."[21]

In the cyber landscape, the changes are dynamic. The evolution of the attack methods and of the required intruder expertise are shown in a graph in Figure no. 2.

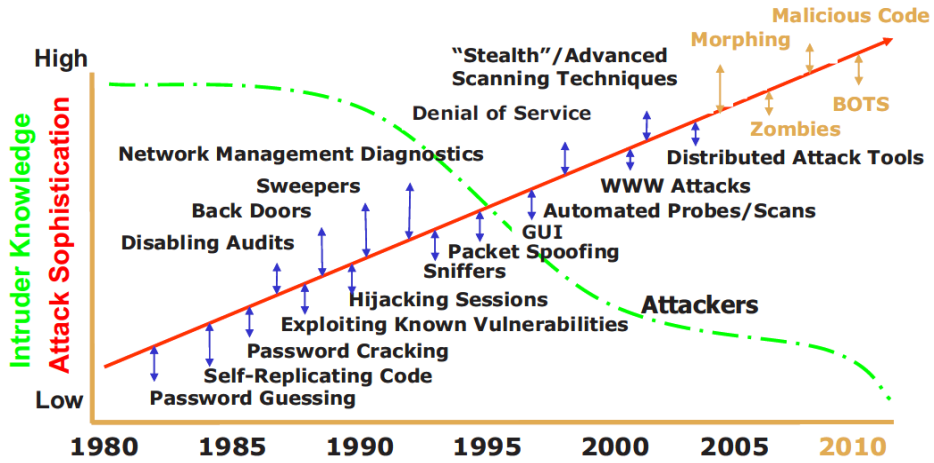


Figure no. 2 The increasing complexity of threats as attackers proliferate[22]

However, the trends of cyber threats, of the tools available for attacks and of the vulnerabilities are evolving at a rate comparable with the most optimistic expectations of revisions to a Design Basis Threat. The annual report of ENISA[23] shows how threats change from year to year, how new concepts emerge.

Evaluation of cyber security measures, or controls, is described in the literature as a mix of compliance check with a list of procedural and, sometimes, technical prescriptions, and structured / quantitative assessments.

While cyber security is defined in the context of cyber systems, which are technical systems, "there is lack of specific technical security metrics research to measure the technical security controls from a total 133 security controls from the ISO/IEC 27001 standard"[24]. Technical measures respond to specific threats and vulnerabilities, which we have found to be rapidly evolving. We consider this to be limiting the cyber system modelling for cyber security purposes, as any model would require real-time update based on new attack methods and newly found vulnerabilities.

A group or researchers at the Idaho National Laboratory proposes an evaluation methodology for risk reduction "based on the assumption that risk is related to the elapsed time required for a successful attack"[25]. The approach considers as a first step the construction of the facility model in terms of cyber elements, with interconnections which are paths towards the final protected elements (vital SCE).

For each element, there are vulnerabilities determined and these are characterized based on the consequence (state of the system element, which becomes a node in a graph

[21] "*Norme privind protecţia instalaţiilor nucleare împotriva ameninţărilor cibernetice*", accessed 15.03.2015, on http://www.cncan.ro/assets/NSC/Ordinul-181-norme-amenintari-cibernetice.pdf

[22] "*Computer Security at Nuclear Facilities*", NSS-17, International Atomic Energy Agency, 2011, p38

[23] "*ENISA Threat Landscape 2014 - Overview of current and emerging cyber-threats*", ENISA, 2014, accessed 15.03.2015, on https://www.enisa.europa.eu

[24] Azuwa, M.P., Ahmad, Rabiah, Sahib, Shahrin, Shamsuddin, Solahuddin, "*Technical Security Metrics Model in Compliance with ISO/IEC 27001 Standard*", International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(4): 280-288, 2012, p. 280

[25] McQueen, Miles, Boyer, Wayne, Flynn, Mark, Beitel, George, "*Quantitative Cyber Risk Reduction Estimation Methodology for a Small SCADA Control System*", Proceedings of the 39th Hawaii International Conference on System Sciences, 2006, accessed 15.03.2015, on http://www5vip.inl.gov/technicalpublications/Documents/3303778.pdf

representation) and type of action (which becomes a path in the graph). Each action has a cost depending on the time required to compromise the element.

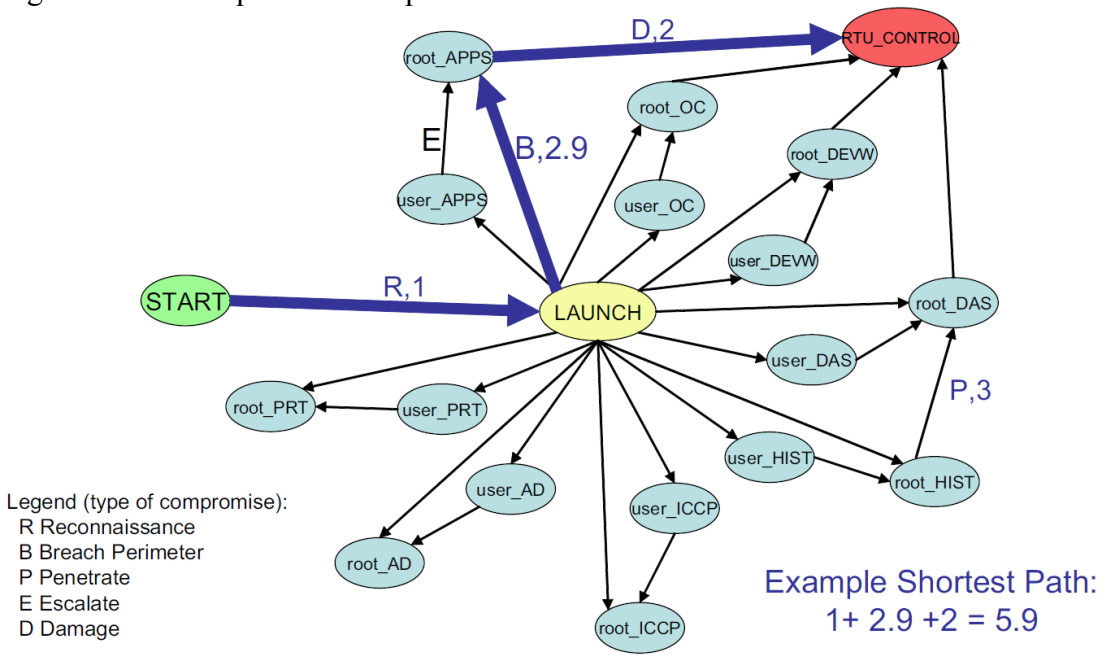


Figure no. 3 Partial compromise graph[26]

Another approach to the evaluation of cyber security systems is the Attack Trees method. The method is credited to Bruce Schneier. "An attack tree is a tree in which the nodes represent attacks. The root node of the tree is the global goal of an attacker. Children of a node are refinements of this goal, and leafs therefore represent attacks that can no longer be refined." [27]

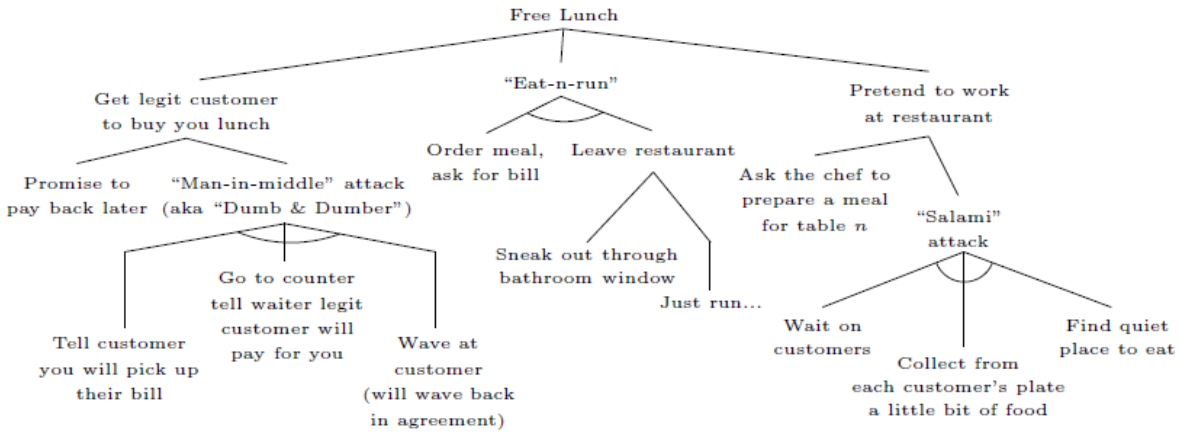


Figure no. 4 Example attack tree[28]

[26] McQueen, Miles, Boyer, Wayne, Flynn, Mark, Beitel, George, "*Quantitative Cyber Risk Reduction Estimation Methodology for a Small SCADA Control System*", Proceedings of the 39th Hawaii International Conference on System Sciences, 2006, accessed 15.03.2015, on http://www5vip.inl.gov/technicalpublications/Documents/3303778.pdf, p. 5

[27] Mauw, Sjouke, Oostdijk, Martijn, "*Foundations of Attack Trees*", Information Security and Cryptology - ICISC 2005, accessed 15.03.2015, on http://web.cs.du.edu/~ramki/papers/attackGraphs/foundations.pdf, p. 1

[28] Mauw, Sjouke, Oostdijk, Martijn, "*Foundations of Attack Trees*", Information Security and Cryptology - ICISC 2005, accessed 15.03.2015, on http://web.cs.du.edu/~ramki/papers/attackGraphs/foundations.pdf, p. 2

Each leaf of the tree represents actions that can be characterized using quantifiable metrics. A further development of this model, which represents a split of attack versus defence characteristics, is the "attack-defence tree" [29].

Conclusions

Although at the moment there is a separation between physical protection and cyber security, both in models and in organizational responsibilities, the literature[30] considers blended attacks for analysis: physical attack, cyber-enabled physical attack, pure cyber-attack and physically-enabled cyber-attack.

We find similarities between the fault tree analysis type of simulation for physical protection and the attack trees and compromise graph models used for cyber security, mainly because they allow to model the attack in a sequential, quantifiable mode.

However, the real-time aspect of cyber security threats and vulnerabilities do not allow for a combined vulnerability assessment that outputs quantifiable results which are usable for long-term security measures planning. Rather than this, we see the output of a combined physical-cyber security assessment tool as a dynamic instrument that allows for detection and security posture adjustment on a continuous basis.

We see potential to develop a unique platform for modelling, assessment and management of the security for nuclear sites, to encompass physical protection and cyber security. Our future efforts will concentrate on developing a model which covers technical, organizational and operational aspects of managing security for nuclear sites in their entire complexity.

BIBLIOGRAPHY:

1. "*SAVI: Systematic Analysis of vulnerability to Intrusion*", Volume 1 of 2, SAND89-0926/1 Sandia National Laboratories, Albuquerque, New Mexico, 1989
2. "*Computer Security at Nuclear Facilities*", NSS-17, International Atomic Energy Agency, 2011
3. "*Design Basis Threat (DBT) Workshop, Session 7, What Could a DBT Look Like?*", DBT Workshop, IAEA, Bucharest, Romania, 2012
4. "*Development, Use and Maintenance of the Design Basis Threat*", accessed 15.03.2015, on http://www-pub.iaea.org/MTCD/publications/PDF/Pub1386_web.pdf
5. "*ENISA Threat Landscape 2014 - Overview of current and emerging cyber-threats*", ENISA, 2014, accessed 15.03.2015, on https://www.enisa.europa.eu
6. "*Guidance and considerations for the implementation of INFCIRC/225/Rev.4, The Physical Protection of Nuclear Material and Nuclear Facilities,IAEA-TECDOC-967 (Rev.1)*", IAEA, 2000, accessed 15.02.2015, on http://www-pub.iaea.org/MTCD/publications/PDF/te_967rev1_prn.pdf

[29] Kordy, Barbara, Mauw, Sjouke, Radomirović, Saša, Schweitzer, Patrick, "*Foundations of Attack–Defense Trees*", Proceedings of the 7th international Workshop on Formal Aspects in Security and Trust (FAST 2010), volume 6561 of LNCS, pages 80-95. Springer-Verlag, 2011, accessed 15.03.2015, on http://satoss.uni.lu/members/barbara/papers/adt.pdf

[30] DePoy, Jennifer, Phelan, James, Sholander, Peter, Smith, Bryan J., Varnado, G. Bruce, Wyss, Gregory D., Darby, John, Walter, Andrew, "*Critical Infrastructure Systems of Systems Assessment Methodology*", Report SAND2006-6399, Sandia National Laboratories, 2006, p. 14.

7. "*Norme privind protecţia instalaţiilor nucleare împotriva ameninţărilor cibernetice*", accessed 15.03.2015, on http://www.cncan.ro/assets/NSC/Ordinul-181-norme-amenintari-cibernetice.pdf
8. "*Normele de Protecţie fizică în Domeniul Nuclear*", accessed 14.03.2015, on http://www.cncan.ro/assets/NPF/npf01.pdf
9. "*Title 10, Code of Federal Regulations, Part 73.1*", accessed 15.03.2015, on http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0001.html
10. "*Title 10, Code of Federal Regulations, Part 73.54, Protection of digital computer and communication systems and networks*", accessed 15.03.2015, on http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html
11. Al-Ayat, R.A., Cousins, T.D., Hoover, E.R., "*ASSESS (Analytic System and Software for Evaluating Safeguards and Security) update: Current status and future developments*", Institute of nuclear materials management conference, Los Angeles, CA (USA), 1990
12. Azuwa, M.P., Ahmad, Rabiah, Sahib, Shahrin, Shamsuddin, Solahuddin, "*Technical Security Metrics Model in Compliance with ISO/IEC 27001 Standard*", International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(4): 280-288, 2012
13. DePoy, Jennifer, Phelan, James, Sholander, Peter, Smith, Bryan J., Varnado, G. Bruce, Wyss, Gregory D., Darby, John, Walter, Andrew, "*Critical Infrastructure Systems of Systems Assessment Methodology*", Report SAND2006-6399, Sandia National Laboratories, 2006
14. Garcia, Mary Lynn, "*The Design and Evaluation of Physical Protection Systems*", 2nd ed. Burlington, MA, Elsevier Butterworth–Heinemann, 2008
15. Gilles, Martin, "*Defending the digital frontier*", The Economist, 12 July 2014, accessed 15.03.2015, on http://www.economist.com/news/special-report/21606416-companies-markets-and-countries-are-increasingly-under-attack-cyber-criminals
16. Heller, Arnie, "*Simulating Warfare Is No Video Game*", Science & Technology Review, Lawrence Livermore National Laboratory, January/February 2000, accessed 15.03.2015, on https://str.llnl.gov/str/pdfs/01_00.1.pdf
17. Jang, Sung Soon, Kwak, Sung-Woo, Yoo, Hosik, Kim, Jung-Soo, Yoon, Wan Ki, "*Development of a Vulnerability Assessment Code for a Physical Protection System: Systematic Analysis of Physical Protection Effectiveness (SAPE)*", Nuclear Engineering and Technology, Vol. 41 No.5, 2009, accessed 15.03.2015, on http://www.kns.org/jknsfile/v41/JK0410747.pdf
18. Kordy, Barbara, Mauw, Sjouke, Radomirović, Saša, Schweitzer, Patrick, "*Foundations of Attack–Defense Trees*", Proceedings of the 7th international Workshop on Formal Aspects in Security and Trust (FAST 2010), volume 6561 of LNCS, pages 80-95. Springer-Verlag, 2011, accessed 15.03.2015, on http://satoss.uni.lu/members/barbara/papers/adt.pdf
19. Kuperman, Alan J., Kirkham, Lara, "*Protecting U.S. Nuclear Facilities from Terrorist Attack: Re-assessing the Current "Design Basis Threat" Approach*", prepared for INMM 54th Annual Meeting, Palm Desert, CA, 2013, accessed 15.03.2015, on http://sites.utexas.edu/nppp/files/2013/07/INMM-2013-July-paper.pdf
20. Malachova, Tereza, Malach, Jindrich, Vintr, Zdenek, "*Threat characterization in vital area identification process*", Proceedings of the 47th International Carnahan Conference on Security Technology (ICCST), vol., no., pp.1,6, 2013

21. Mauw, Sjouke, Oostdijk, Martijn, "*Foundations of Attack Trees*", Information Security and Cryptology - ICISC 2005, accessed 15.03.2015, on http://web.cs.du.edu/~ramki/papers/attackGraphs/foundations.pdf
22. McQueen, Miles, Boyer, Wayne, Flynn, Mark, Beitel, George, "*Quantitative Cyber Risk Reduction Estimation Methodology for a Small SCADA Control System*", Proceedings of the 39th Hawaii International Conference on System Sciences, 2006, accessed 15.03.2015, on http://www5vip.inl.gov/technicalpublications/Documents/3303778.pdf
23. Miller, Bill, Dale Rowe, "*A survey of SCADA and critical infrastructure incidents*", Proceedings of the 1st Annual conference on Research in information technology, ACM, 2012
24. Whitehead, Donnie, Potter, Claude, O'Connor, Sharon, "*Nuclear Power Plant Security Assessment Technical Manual*", Sandia Report SAND2007-5591, 2007, accessed 15.03.2015, on http://prod.sandia.gov/techlib/access-control.cgi/2007/075591.pdf

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"."*

GENERAL ISSUES RELATED TO RISK MANAGEMENT WITHIN INFORMATIONAL ENVIRONMENTS

Dănuţ NECHITA
PhD student in the field of Public Order and National Security, forensic trainer within "ALEXANDRU IOAN CUZA" Police Academy, Bucharest, Romania,
e-mail: danut_nec@yahoo.com.

Georgică PANFIL, PhD
Georgică Panfil, PhD in the field of Public Order and National Security, lecturer within "ALEXANDRU IOAN CUZA" Police Academy, Bucharest, Romania, e-mail:
panfil.george@gmail.com.

Abstract: *The article presents the main aspects related to the processes associated with efficient risk management in the environments related to the information technology. The authors are tackling the successive steps of the risk analysis, risk measurement and risk characterization. Furthermore, the conclusions are focused on the idea of best practices and methods to mitigate risks, focusing especially on the public institutions in which the environment contains sensitive intelligence and data.*

Keywords: *risk management, security, mitigation, risk.*

At the level of every type of institution, the cyber-environments have a definite and sensitive role. Nowadays in every organization one can identify one or multiple links between its goals and one or more IT systems. From our point of view, every manager must be aware of the challenges related to the main categories of risks with origins in the field of cyber environments, especially due to the fact that this type of environment can represent a source of threats or one for internal systemic flaws.

1. Risk management fundamentals

Every organization has some specific predefined objectives. Sometimes some uncertainties might occur in direct consonance with the possibility to achieve those objectives. It does not matter the type of those objectives, but it is obvious that when the uncertain appears, the efficiency is seriously questioned. Thus, we can talk, in the above-described situation, about a risk. We can present various definitions of the idea of risk, but one of the most accepted of them describes risk as the probability of threat of quantifiable damage that is caused by internal vulnerabilities or external threats. In the view of International Standardization Organization, risk is defined as "effect of uncertainties on objectives", or such as "the probability of uncertain future events" (ISO 31000 Standards Collection – Risk Vocabulary)[1]. No matter the approach taken on this definition, we shall conclude the fact that risk have the following components:

-an internal *vulnerability* of the organization;
-an external *threat*;
-a quantifiable *impact* on the organization's assets;

[1] ISO Standard 73:2009 Risk Management Vocabulary – www.iso.org and www.iso-standards.org.

-a *probability f*or the event to occur (either from the point of view of the vulnerability, the threat or both).

The vulnerability defines the internal component of the risk and refers to states of fact, processes, individuals, phenomenon from the inside of an organization that can diminish its capacity of reaction to the potential or existent risks or that are favoring the occurrence or development of a risk. In other words, a vulnerability means every characteristic of a system to be easily attacked, to have sensitive parts. No matter the definition, the vulnerability defines the internal element of a risk.

The threat represents the action, inaction, phenomenon, process or individual, able to cause a loss or an impact to an organization. The threats usually have an external source and must not be misaddressed with the concept of vulnerability.

From the point of view of the researchers in the field of risk management, the combination between threats and vulnerabilities provides the risk environment and the parameters of risk occurrence. If one of those have a probability of occurrence near zero, risk itself is almost nonexistent. Furthermore, when an institution is in presence of a threat, but that threat has nothing to exploit, there is no impact, thus the potential risk is nonexistent (let us imagine the situation in which we can talk about a computer virus as a threat, but we have an organization without computers - thus an unexposed one).

When a risk occurs, the manager will have to take a decision, which is either to transfer the risk, to reject it, to reduce it or to accept it. Either one to there options has different implications, such as taking different sets of measures (eliminate the vulnerability or the source of threat, increase the general preventive measures, taking no measures in some cases etc.). However, in order to have the concrete possibility to understand what your are dealing with, risk analysis/evaluation is needed (the process of a risk characterization, from the point of view of its components, it's architecture, it's variables - vulnerabilities exploited, threats' source, probability - from a mathematical and statistical point of view etc., all of those together with descriptive elements and theories). It has to be said that this task is to be carried by a risk analyst, usually not the same person with the manager itself. As follows, realizing an organizational risk profile and determining the degree of risk exposure should be a continuous preoccupation of the manager.

To sum up the previous statements, we can also provide a definition of the risk management itself. Thus, risk management refers to all the procedures, decisions and measures taken by the manager in order to identify vulnerabilities, threats, risks, best mitigation methods and best options to prevent or at least diminish risk impact. The process or processes associated to risk management can be developed by one person or more, be there the manager/ management team or analysts dedicated to this domain. Should the risk management workflow be developed by the analyst, the management layer will be involved thru the decisions that are to be taken.

The main characteristics of the risk management process are underlined thru the concepts expressed by International Organization for Standardization (ISO) within ISO 31000 Standards Collection[2], as follows:

-it creates value, based on the principle that the expenses related to the risk management should be lower than the impact of the unattended risk;

-risk management is directly integrated within all the processes developed at organizational level;

-it is an important component of the decision making process;

-it explicitly addresses uncertain concepts such as probability and possibility;

-it is a process organized on different layers and steps;

[2] International Standards Organization, ISO 31000 Collection – www.iso.org.

-the risk management process must be supported by a very well structured documentation;

-the risk management process should be calibrated on the organizational needs;

-it is based on the evaluation and action of human factors;

-it is a transparent process, at least from some points-of-view;

-it must be an adaptable workflow;

-it must allow periodically reassessments[3].

2. Risk evaluation for IT systems – an essential step of the risk management itself

First step for an efficient risk management workflow dedicated to cyber environments is the one related to risk evaluation. Usually, this phase is intended to provide an image of the dimensions of a threat ant its characteristics, as those characteristics will be exploited in the following phases for risk mitigation or elimination.

Risk evaluation is composed from nine fundamental segments, as follows:

-environmental description and characterization;

-threat identification;

-vulnerability identification;

-analysis of control and prevention methods;

-determining possibility and probability;

-impact analysis;

-risk determination;

-elaborating proposals for the future controls;

-documenting the results.

It has to be said that the order of the activities described above is not mandatory, as some of them – such as threat/vulnerability identification and controls analysis can be realized simultaneously, while system characterization and documenting the results are initial and, per se, final activities.

2.1. System characterization

Evaluating an information technology system is based on understanding how it works and which are the main workflows and functions of that system. As such, the fundamental components and resources of the system must be identified[4], as well as the data contained by the system.

One of the most important aspects related to the system characterization is the one related to data gathering. The following types of data will be taken under consideration:

-elements related to the hardware and software (system characteristics, providers, developers, software versions, update policies etc.);

-internal and external connectivity of the system;

-list of accounts providing access and the type of access for every user;

-main purpose of the system;

-the value of the system;

-level of required protection in order to maintain the system integrity, availability and confidentiality;

-other data, such as security policies, network diagrams, workflows, controls, physical security etc.

[3] NIST Standard SP 800-30, 800-37 and 800-39 – www.crc.nist.gov.

[4] NIST Standard 800-37 (www.crc.nist.gov) Guide for Applying the Risk Management Framework.

2.2. Vulnerability identification

As stated before, vulnerabilities are those flaws in the systemic security. In order to obtain a viable list of vulnerabilities exploitable by external threats, it is recommended to access different information sources, system testing and verifying some of the data resulted from system characterization.

The sources of vulnerabilities will be tackled differently, depending of the system state[5]:

-for operational systems, identifying vulnerabilities will focus on the effective analysis of the system, as well as the measures already in place meant to protect the system;

-for systems already designed, being under the implementation phase, the search for vulnerabilities will be concentrated on the policies related to the implementation and on the existent schematics, together with the existing certifications and previous tests[6];

-for systems under the design phase, searching for vulnerabilities will be developed concentrating on the general policies of the institution, procedures, regulations, previous analysis, and, if case, technical characteristics of the system.

Some advantages related to the vulnerability identification can be retrieved from system testing, using different testing methods, such as automatic scan for vulnerabilities, security tests or penetration tests (port scanners, database scanners, simulations etc.).

2.3. Threat identification

Within this step, the activities are focused on the possible sources to exploit the flaws of the informational system, as well as establishing the motivation or, if case, the effective manifestation of such sources. Directly related to the subject of this article, a threat for the IT system can be any circumstance or event with potential to affect the system. The most common threats can have human, natural or environmental origins. It is obvious that human factors are the most important ones to consider, yet the others should not be neglected – storms, earthquakes, electrical storms, pollution etc.

From the point of view of the threat`s motivation, it is obvious that this can only be tackled only referring to the human factor – as such, humans are the most serious source of threat. It is a must to separate the possible persons with intentions to harm using taxonomies related to the environment they are coming from, their purpose etc. One must not neglect the previous personnel that worked within the institution (due to the knowledge related to the system itself), possible cyber terrorists, ordinary cybercriminals, as well as simple hackers, motivated only by the desire to by-pass a firewall or to achieve fame from gaining control to a government`s website.

2.4 Analysis of controls and preventive measures

The purpose of this segment is to eliminate the inner flaws of previously implemented measures from the system. On the other hand, one must not neglect the preventive measures that are predicted to be implemented at a certain time in perspective. If there are no such measures implemented, the need for implementation must be underlined and brought into the attention of the management layer. The preventive measures can be either technical ones (incorporated within the hardware, software or firmware) or procedural/operational ones (security policies, operation procedures, internal regulations etc.).

---

[5] Georgică Panfil, – *Risk management related to informational security*, Estfalia Publishing House, Bucharest, Romania, 2013, p. 27.

[6] Urs E. Gattiker,– *Information security, strategies for understanding and reducing risks*, John Wiley & Sons, 2005, p. 87.

2.5. Determining probability

Within this phase the main purpose is to obtain a rating of the possibility that a certain vulnerability to be exploited by a certain threat. As such, the following factors will be taken under consideration:

-the motivation and the capacity of the threat source of being dangerous for IT system/organization;

-the nature and the characteristics of the vulnerability;

-the existence and the efficiency of the prevention/control measures.

The conclusions of this phase will be presented on an qualitative scale, with the possibility of being high, moderate or low, directly related to the threat`s motivation degree and the measures already implemented.

2.6. Analysis of the potential impact

It is very important to understand how much damage can be inflicted by a certain incident. As such, one should consider aspects related to the importance of the information system for the institution, system`s and processes` destination and of course system`s sensitivity (the required protection level for the system in order to maintain its CIA trinome). Hence, the analysis will evaluate the system from the following points of view: loss of integrity (unauthorized modifications), loss of availability (should the system be essential for the organization`s goal, losing the possibility to access it means endangering organization`s fundamental purpose) and loss of confidentiality (failure to protect data from unauthorized access).

The potential impact should be characterized as follows:

-high (it seriously affect the institution itself with its goals, human resource and values);

-medium (it creates great financial damage and can also induce harms for human resource);

-low (it creates some financial losses and minor losses for the organization itself).

2.7. Determining risk level

This task is based on previous gathered data within the others segments of the evaluation and is meant to reflect the level of risk associated to the IT system[7]. Risk determination for a pair of vulnerability-threat can be expressed related to:

-the possibility that a given threat source will exploit a given vulnerability;

-the dimension of the impact or the effects following the successful exploitation of a vulnerability from a threat;

-the estimated efficiency of the prevention or at least detection mechanisms implemented for risk reduction or risk elimination.

In order to measure risk, different instruments such as risk matrix, eventually followed by risk scales, can be used.

2.8. Recommendation of anti-risk measures

Following the workflow developed until this point, measures capable to diminish or even eliminate the identified risks can be elaborated. Their purpose is to reduce the level of risk for an informational system and its contained data to an acceptable level[8]. However, one should take into account the following issues related to those measures:

-the compatibility with the system`s or organization`s realities;

-law or regulatory limitations;

---

[7] NIST Standard 800-39, Managing Information Security Risk – www.crc.nist.gov.

[8] Doug Howard, – *Security 2020, reduce risks this decade*, Wiley Publications, 2010, p. 112.

-organization`s policies;
-operational impact;
-safety/security provided by the proposed measures.

It has to be said that, from our point of view, the phase of measures recommendation is one of the most important results of the risk evaluation (assessment) and it is meant to provide a solid base for the risk mitigation process, during which the procedural recommendations, as well as security measures are evaluated, prioritized and implemented.

2.9. Documenting the results

Documenting results represents the final phase for risk evaluation and is related to the report containing the results and the noted observations. The purpose of the report is to provide a sustainable help to the decisional layer in implementing the operational, financial, procedural and regulatory changes. This type of report is not related to the shape of an audit report, which sometimes tends to contain rather harsh-objective terms, but rather of a more systematic manner and analytical too, providing the management layer an instrument to a better understanding of the evaluation an of a better decision-making process.

The report will contain the following aspects[9]:

-introduction part (evaluation purpose, objectives, system description, components description, users, locations, infrastructure etc.);

-brief presentation of working methodology, participants, techniques used for evaluation, types of matrix etc.

-system characterization from the point of view of hardware, software, interfaces, data, users, policies, diagrams, graphs etc.

-description of vulnerabilities and risks;

-presentation of the results of evaluation, risk rating, recommended measures, impact type and amplitude etc.

-conclusions.

Conclusions

Current article is concentrated on the issues related to risk management and focused – thru the case study as the main research method – on the risk evaluation concerning an information technology system, be there computer or network or other informational asset. We consider that every managers should be aware of the main phases related to risk evaluation and the best practices to be followed as such. It is obvious that, in the current context, every organization should keep an eye on the risks that tend to threaten it, and especially the ones related to the safety of cyber components.

Elimination or diminishing of risk related to cyber environments is an important step in achieving of the organization`s objectives. Thus, a management policy related to proper handling of risks brings many benefits to the organization, from both economic and operational points of view.

[9] NIST Standard 800-37 (www.crc.nist.gov) Guide for Applying the Risk Management Framework.

BIBLIOGRAPHY:

1. Doug, Howard – Security 2020, reduce risks this decade, Wiley Publications, 2010.
2. Georgică, Panfil – Risk management fundamentals, in European Journal of Public Order and National Security, issue 3/2014.
3. Georgică, Panfil – Risk management related to informational security, Estfalia Publishing House, Bucharest, Romania, 2013.
4. ISO 31000:2009 Standard (www.iso.org) - Principles and Guidelines on Implementation
5. ISO Guide 73:2009 (www.iso.org) - Risk Management - Vocabulary
6. ISO/IEC 27000 Standards (www.iso.org) - Information technology — Security techniques — Information security management systems — Overview and vocabulary.
7. ISO/IEC 31010:2009 Standard (www.iso.org) - Risk Management - Risk Assessment Techniques
8. NIST Standard 800-30 (www.crc.nist.gov) - Risk Management Guide for. Information Technology Systems
9. NIST Standard 800-37 (www.crc.nist.gov) Guide for Applying the Risk Management Framework
10. NIST Standard 800-39 (www.crc.nist.gov) Managing Information Security Risk,
11. Urs .E., Gattiker – Information security, strategies for understanding and reducing risks, John Wiley & Sons, 2005.

COMMUNICATION OF TERROR IN CYBERSPACE

Dragoş Claudiu FULEA
Romanian Intelligence Service, e-mail: dfulea870@dcti.ro

Cătălin MIRCEA
Romanian Intelligence Service, e-mail: cmircea870@dcti.ro

Marius Ciprian CORBU
Romanian Intelligence Service,, e-mail: mcorbu870@dcti.ro

Abstract: *From the point of view of technical facilities offered, WEB 2.0 is an ideal space for the manifestation of terrorist organizations of the intent of organizing operations, claiming attacks or promoting their ideology. Lately, in cases such as that of the so-called Islamic State of Iraq and Syria (ISIS) we witness a mutation in the communication registry through translation of the message towards an explicit and illustrative form of terror. From this view, should not be omitted any risk that increased addiction among the youth segment, even the one with a high level of training for the Western targeted countries, of strong negative emotions generated by the posts with an increased degree of violence, spread by media products with a global audience, could favor a gain in popularity of the ISIS video "productions". On the other hand, the colossal strength of the communication specific to New Media age might be able to accelerate the process of online indoctrination intended by terrorists.*

The paper aims to explore the evolution and impact of the terrorist message in cyberspace, constituting, as well, in a plea for an IT&C technological superiority on behalf of the intelligence services that, along with the human resource training, may lead to an increase in the efficiency of the reaction against the terrorist threat.

Keywords: *Terrorist WEB, New Media, IT&C, intelligence services, WEB 2.0.*

Introduction

World public opinion is still beset by media operators, with stereotypical clichés of terrorists from the Middle East like this: mentally violent alienated marked by poverty, equipped with rudimentary means of communication and battle.

Also, the quasi-existence of an integrated analytical approach within the assessment and creative process regarding the message disseminated to media on a global basis has increased the schematic, confuse perception with negative connotations on this geographical area regarded as a traditionalist, inner world, which rejects any contemporary values. Thus, the extremist movement, Islamic State of Iraq and Syria (ISIS) became the new Middle Eastern media label.

Undeniably, the reality of the Muslim countries of the region is crossed by various violent fundamentalist orientations and one of the reasons of ISIS implantation lies in the weakness or even the exhaustion of countries bordering the limit of a failed state index, marked by military conflicts, foreign (Iraq) or internal (Syria, Libya).

In the case of the Islamic State of Iraq and al-Sham (ISIS), a succinct analysis of the organizational profile reveals a surprising alternative reality, such as:

- The existence of deep political motivations strong enough to be able to distort the religious ideals and cynically make use of the devotion and fervor specific to this Millenary religion for violent purposes;
- Socially heterogeneous, composed of various segments of the population;
- Multinational pattern which spreads on a regional level with higher risk to broadcast internationally;
- Important IT&C capabilities, engaged in a thoroughly elaborated approach of disseminating online an illustrative and explicit form of terror;
- Training in the military field - solid knowledge, both theoretically and practically, in military tactics, especially guerrilla fighting in urban areas.

In this setting, it becomes obvious the Middle East' Muslim countries' efforts to conceal the fundamentalist-terrorist contagion effect, to the territory presently occupied by ISIS.

The paper aims to explore the evolution and impact of the terrorist message in cyberspace, constituting, as well, in a plea for an IT&C technological superiority on behalf of the intelligence services that, along with the human resource training, may lead to an increase in the efficiency of the reaction against the terrorist threat.

1. Communication in Cyberspace

The Internet offers the possibility of conducting interactive communication; the transmitter can better direct the flow of communication and orient it towards the targeted receiver. Thusly, each user is capable to send messages to multiple receivers, which, in turn, may render the message as received. The end is that each participant in mass communication on the Internet is both transmitter and recipient.

Nevertheless, intensive use of the technological platforms offered by the Internet has increased the depth of the mass communication process with new elements such as instant feedback and the ability to respond using the same channel as the sender, but also using additional channels.

In this context, it can be assessed that although the fundamental communication trinomial sequence remained unchanged (transmitter - communication channel - receiver), the technological revolution of the transmission channel has led to significant changes that shaped the model of communication from linear (classical) to a molecular shape.

It is difficult to appraise a precise definition of New Media as it relates to a wide range of references and a fluid, continually evolving domain. A particular understanding of the term useful for this article refers to the multiple forms of electronic communication that are made possible by the existence of the technological platform called Web 2.0.

Social media is the most successful proponent of the social interactivity of the online environment and, also the main component of New Media Philosophy.

Elements of the cyberspace representative of what is called New Media include:

- Blogs;
- Discussion Forums, message boards and chat rooms;
- Social networks;
- Instant messaging (messenger type applications);
- The new reality within the virtual worlds;
- The integration of mobile telephony into the digital space (Smartphone, PDA, PC tablet).

The amplitude of the propaganda disseminated through New Media specific information and communication tools should not be underestimated. The most representative

example is the use of social media in the onset and development of the "Arab Spring" or passing around the hate message of ISIS.

If there is any trace of skepticism to this statement would be sufficient a short consultation within the Facebook' page *We are all Hamza Akhateeb*, which is broadcasting, multimedia related to serious abuses committed by the regime in Damascus against the civilian population or the ones affiliated with the Islamic State of Iraq and al-Sham.

2. WEB 2.0 Terrorism

In terms of technological facilities offered, WEB 2.0 is an ideal event space for terrorist groups for several reasons, among which include:

- Fast access;
- Increased user interactivity;
- Vast audience made up of people from across the world;
- Relative anonymous communication over short periods of time;
- Approach to a fast flow of data;
- Limited financial resources;
- Multimedia communication possibilities;
- Precariousness regulations, censorship or other kinds of government restraint;
- Source of data for journalists which are employing traditional media WEB 1.0 type.

Exploiting these features provided terrorist organizations, particularly jihadist ones acting in the Middle East, the possibility of control over the distribution of propaganda messages intended for broad classes of receptors.

In this connection, Muslim extremists have consolidated the use of WEB 2.0 resources as a virtual agora, free of constraints on nationalities and borders, integrating and promoting extremist currents of opinion for the auditorium of electronic publications that provide religious, ideological and military training for jihadists.

On the other hand, essential elements of New Media, such as Twitter, WhatsApp, Facebook, YouTube are widely used by jihadi activists, especially the ones supporting ISIS.

Further studies[1] have shown that only in a limited time period (September to December 2014) Islamic State activists have exploited a considerable number of active Twitter accounts estimated between 46.000 to 70,000, localized by GPS mainly in Iraq and Syria, but also in countries such as Saudi Arabia, Egypt, Tunisia, Libya, Yemen and the Gaza Strip[2].

Is to be noted that that the popularization of ISIS on the aforementioned social platform has been caused by a small group of users, between 500 and 2,000. Figure no. 1 is the graphical representation of the communication process enabled by the "tough core" of ISIS network activism on Twitter. The assessment of the growth of the ISIS base of supporters on Twitter, revealed more, interesting aspects such as the possibility of documenting the ideological rift between ISIS and Al-Qaida. Many supporters of Al-Qaida have abandoned the accounts created before the year 2010 and have recreated others to prove their loyalty to ISIS.

[1] J.M. Berger and Jonat hon Morgan, "The ISIS Twitter Census. Defining and describing the population of ISIS supporters on Twitter", The Brookings Project on U.S. Relations with the Islamic World, analysis paper March 2015.

[2] Aaron Zelin, "The Islamic State's Model," *Washington Post*, 28 January 2015, http://www. washingtonpost.com/ blogs/monkey-cage/wp/2015/01/28/the-islamic-states-model.

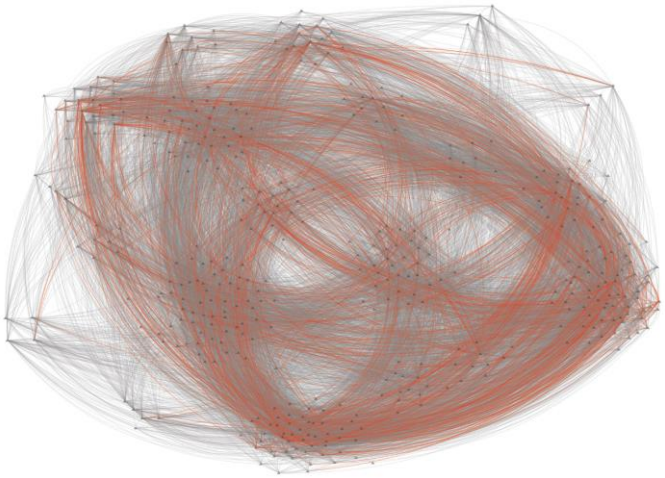


Figure no. 1

Recently, the increase of toxic communication of terrorist genesis within cyberspace continues to favor the spread of a dangerous phenomenon, namely the spontaneous generation of terrorist cells whose members may meet ad-hoc in order to carry on the terrorist operation, without previous common training, subsequent to communicating in private encoded chat rooms. The unfortunate premiere of this nefarious type of activism, opened in July 2005, through the London attacks, risks to exponentially multiply in the future.

Secondarily, from technological and managerial perspective, WEB 2.0 has facilitated a qualitatively superior operational coordination in the activity of terrorist entities. For example, to secure communication, both with their own cells and the potential candidates for recruitment, terrorist groups have turned to public available encryption software with exponential key, such as Pretty Good Privacy (P.G.P.), which allowed encoding mail traffic that disseminating data on weapons, targets and combat tactics.

Furthermore, terrorists have consolidated the use of steganography, a technique involving concealment of messages (instructions as maps, photographs, directions and technical details about using explosives) inside of graphic files (eg images containing sexually explicit material emailed between Muslim extremists). There are clues that lead to the conclusion that the authors of the bloody terrorist attacks in Paris against the Charlie Hebdo comic magazine have used steganography. French investigators have identified, in 2010, within the computers belonging to Amedy Coulibaly (self-confessed supporter ISIS) and Cherif Kouachi (self-confessed supporter of Al-Qaida) files with child pornography, which actually dissimulated the use by the two terrorists of the messaging sites for adults, in order to avoid detection by the authorities[3].

3. Terrorist Communication Components

Broadcasters

The presence of terrorist groups on the Internet has several consequences, including the threat to the stability and credibility of information sources (increased risk of occurrence of cases of deception and fraud) and the increase in numbers of members supporters and sympathizers not only in the country of origin, but also in distant countries.

Typically, websites contain terrorist organization's history and activities, a detailed analysis of its social and political formation, biographies of leaders, founders, heroes, data about its political aims, ideological, criticism on foes, daily news.

[3]http://tempsreel.nouvelobs.com/charlie-hebdo/20150114.OBS9988/info-obs-les-cliches-pedophiles-une-couverture-pour-coulibaly-et-kouachi.html

Message

Until the beginning of the first decade of the present Millennium, most terrorist sites did not present detailed descriptions of criminal actions and their catastrophic consequences. This strategy was in line with the propaganda and the construction of the image that the terrorists had planned to present to potential supporters through the Internet.

Currently, broadcast messages on social networks or websites owned by terrorist organizations such as the Islamic State of Iraq and ash-Sham presents a high level of refinement. Is to be noted that the broadcasted messages on social networks or websites owned by terrorist organizations meet the specific communicational structure of a complex operation originated initially in the domain of intelligence, sequenced on three distinct stages: propaganda, countering propaganda and influencing, at the same time with a exacerbated violence in the communication through translation of the message by an explicit and illustrative form of terror.

The first rhetorical structure contains pure propaganda and promotes the concept of lack of alternative but armed struggle (attention, it does not use of the term "violence") viewed as a last resort where the "weak", "poor" and "helpless" can successfully oppose the "strong", "rich" and "resourceful".

While criminal acts orchestrated by terrorists against civilian populations that is not sharing the same “”truthful faith” are not observed, the countermeasures taken by governments and regimes that oppose terrorism are characterized by terms such as "genocide", "mass murder" or "bloody massacre."

The terrorist organization is presented as a subject of persecution, with leaders hunted down and assassinated, members and supporters massacred all in order to deter the freedom of religious expression or state self-determination (The Islamic Caliphate).

Intentionally the message focuses on terrorism opponent's intention to limit freedom of expression and the right of self-determination of the "weak" which is defended only by the "freedom fighters" i.e. terrorists. The reason is to confuse the targeted public since these concepts are well anchored in the Western Euro-Atlantic collective mentality, with strong cognitive symbolic resonance for both Europeans and North Americans.

The second rhetorical structure aims to counter the “enemy” propaganda and represents a set of measures for cosmetizing the terrorists' violent motives.

In practice, the most commonly used method is to use and promote within social media a non-violent language. The message broadcasted into the social networks is distorted and manipulated for the purposes of falsely asserting as a final objective of the terrorism the so-called "peaceful settlement" by "diplomatic negotiations" under the conditions that nations that oppose terrorism should accept the political solution of ISIS.

The last rhetorical structure aims at influencing and sensibilizing the potential adepts from the youth section of society that is accessing terrorist websites, as a preliminary grading and selection for recruitment. It involves careful planning of how to develop and phase the message which is disseminated, at first, in a unidirectional manner.

Not surprisingly, despite the technological advances of the communication channel the terrorist propaganda is using an archaic method which remains still effective: the demonization and lack of legitimacy of the enemies.

In this stage, the message contains aggressive, violent and expressive linguistic constructions as it needs to lash out in a negative manner the registry of primary emotions, namely the individual's sense of belonging to a religion as a condition of human mental and moral stability. In that sense, the communication broadcast a warning on defending religious values of belonging against the danger of extinction caused by "enemy" actions.

Recently, this message has been amplified by the dissemination of malicious, extremely violent videos within the cyberspace. ISIS' hostage executions draw media like a

magnet and satisfy a perverse desire for blood and sensational as well as contempt towards human values.

On the single hand, the slow-motion replay of the moment of unloading the firearm into the victim's brain, as easily as the obsession for visual details of the wounds to the brain and the repose of the body it intends to locate a mental anchor to the spectator. Basically, ISIS intends to associate the image of its fighter as a holder of power, judge and executioner above life or death. On the other hand, the dissemination of ISIS executions by decapitation has an uncontrollable media potential, terrorists becoming addicted to posting increasingly disturbing details to keep online rating higher and attracting so, new followers (e.g., burning alive of the Jordanian pilot imprisoned in a cage).

Receptors

It must be underlined that the younger segment of the population, predominantly in the Muslim area of influence, which is the primary object of terrorist organizations acting in the Middle East is as permeable and influenced by the toxic communication message of terrorist genesis, just as the Western youth, due to the permanent connection through new media tools as Smartphones and PC tablets, running on the platform offered by WEB 2.0 technology.

Online audit studies have proven that the Islamic State supporters used in proportions of 69% Smartphones with Android operating system, 30% use IOS and only 1% Blackberry.

Oftentimes, the arrangement of receptors of the toxic communication of terrorist genesis follows the form of concentric bands. Firstly, the terrorist group will target as receptors the local champions, creating for them a local language site that will incorporate detailed data on the organization's actions and domestic policy, on allies and enemies. Secondarily, the following outer circle will reach the international public opinion, which is not directly involved in the conflict, but that might be interested in this topic. In this case, the site is developed in languages other than the one currently spoken by terrorists. Websites are mainly in English, for an internationally broadcasting. For this type of receptors web pages include only basic information about the organization.

The last outer circle of receptor concerns the public considered as an enemy (citizens of the nations that fight against terrorist groups). Site content is not explicitly made for this kind of audience, but there are web pages which make obvious efforts to demoralize the enemy public by threatening with terrorist attacks and trying to engender a sense of guilt regarding the motives and actions of the antiterrorist troops. Another purpose is to stimulate public debate in enemy countries, to change public opinion and undermine public support for the government of the target state.

A new and extremely dangerous element, introduced by ISIS activism who particularizes this organization consists of filtering out the public within the European, American or Asian countries, members of the anti-terrorism coalition. The targeted population segment is represented by teenagers coming from the second generation of Islamic immigrants originating from areas of conflict, settled in the countries that have provided sanctuary.[4]. They pass most of their time online, acquiring new information about the early culture and inheritance of their parents or regarding the social, political and economic developments from the original home lands. In this context, they can become vulnerable to the aggressive fundamentalist religious propaganda militancy and afterwards susceptible to adherence to acts of violence, motivating this approach by the desire to recover the apathetic "older generation", corrupted by the welfare provided by the standard of livelihood in the host nations. There are targeted mainly Western states, which have offered sanctuary.

[4]http://www.independent.co.uk/voices/comment/isis-in-the-uk-how-the-war-on-terror-radicalised-a-generation-9813362.html

In this respect, it can be appreciated that the finality of ISIS approaches is aimed to obtain an overwhelming support from the behalf of the Ummah, the global Islamic community of all Muslims.

4. WEB 2.0 Terrorism vs. Intelligence

As may be concluded from the previously presented situation, the challenges of WEB 2.0 terrorism (including terrorist communication over New Media) to the intelligence activities are numerous and difficult to address.

Experience has shown that in order to anticipate terrorist threats the intelligence agencies have the most difficult task in absorbing, processing, going through the analytic filter an enormous volume of data, in order to produce, deliver and disseminate a valid intelligence product to the policy-makers.

The documentation, preparation and coordination of the logistical, fiscal and human resource involved by a terrorist operation are hard to identify and curb as their "signature" on WEB 2.0 is diffuse. On the other hand, too many times the intelligence collected doesn't fill the pattern of a threat in time.

Therefore, gaining a technological superiority as well as training the human resource was the only appropriate measure.

In this context, the intelligence communities' response has been focused on development and specializing analytic capabilities, while equipping them with IT&C (information technology and communication) tools able to identify in due time credible terrorist activities "signature" within the virtual space which can result in terrorist acts. Especially in case of a failure of preventive measures, the intelligence product must be updated and presented to the policy makers in order to take the appropriate measures to limit the collateral effects of the attack.

For example, in practice, during the "classic" process of assessing intelligence products that meet all the requirements to be disseminated to the policy makers, intelligence analysts consume a disproportionate time between research, analysis and production phases.

Thus, most of the time is allocated to data research (search, visualization, collection, reading and pre-processing of data in order to build an assessment) and to a lesser extend for data analysis (formulation of correct, real and verifiable assessments), precisely the phase which defines the value of the intelligence product.

Several experiments conducted on international level aimed at acquiring the analytical capabilities by implementing information technology have undoubtedly proven that using IT&C tools have contributed to an impressing increase in the caliber of the news product. Moreover, the time allocated to the research period has been drastically cut back, which granted an appropriate time for refining and certifying the analysis.

IT&C tools for cooperation, support within the intelligence communities, as well as those ensuring decision supports for the policy makers allow the man-machine team to analyze and solve complex informational problems, efficiently and timely. The big winner of the use of these tools lies in transforming huge volume of data that often tends to overburden analytical capabilities of the intelligence and security services in what could be called intelligence precursors.

Why to be called intelligence precursors and not intelligence? Since ultimately only human element can turn data into information and information into knowledge. IT&C tools can only amplify the capabilities of the human intellect. In the area of terrorism prevention, addressing a problem by using information technology is allowing the analyst to avoid mental traps generated by biases or errors caused by limited data input.

Conclusions

The assessment of ISIS message in cyberspace unveils that organization has developed an elaborated construction, which far exceeds the proportions of a terrorist group, which is carefully overlapped on the primordial example of Islamic faith, in order to satisfy the demand of religion. In fact, the "Islamic Caliphate" is a potentially huge promotional offer: on one hand, provides a new horizon of hope for local Muslim populations in terms of the failure of the "Arab spring", and on the other hand takes off a desperate cry for backing from the World Islamic community.

It would be wrong to assume that New Media is the cause of the spread of the global terrorist phenomenon. It can only be concluded that the information technology revolution has put into motion all the intimate resorts and manifestations (beneficial or not) of the human society, in its effort to adapt to a globalized environment .

As for the intelligence communities the major problem lies not in the online collection of intelligence, but how to transform intelligence in knowledge and action, concomitantly finding pragmatic answers to two questions:

- What data and information collected in the digital space is truly relevant?
- What is the best way to analyze and transform relevant data into valid intelligence products?

BIBLIOGRAPHY:

1. COMAN Daniela, „*Comunicarea în cadrul proceselor specifice fenomenului terorist”*, Bucureşti, SNSPA, 2007;
2. DELCEA Cristian, „*Psihologia terorismului: studiu psihologic asupra teroriştilor”,* Cluj-Napoca, Editura Albastră, 2004;
3. http://tempsreel.nouvelobs.com/charlie-hebdo/20150114.OBS9988/info-obs-les-cliches-pedophiles-une-couverture-pour-coulibaly-et-kouachi.html;
4. http://www.huffingtonpost.co.uk/david-churchill/radical-islam_b_6115138.html;
5. http://www.ibtimes.co.uk/when-isis-jihadists-return-home-how-de-radicalise-islamic-extremists-1474905;
6. http://www.independent.co.uk/voices/comment/isis-in-the-uk-how-the-war-on-terror-radicalised-a-generation-9813362.html;
7. http://www.washingtonpost.com/blogs/monkey-cage/wp/2015/01/28/the-islamic-states-model;
8. KAPLAN, Eben, „*Terrorists and the Internet”,* Council on Foreign Relations, May 2004, accessed în 15 martie 2015 la http://www.cfr.org/publication/10005;
9. POPP Robert, ARMOUR Thomas, SENATOR Ted, NUMRYCH Kristen, „*Countering terrorism trough information technology, Comunications of the ACM*”, vol. 47, no. 3, Minneapolis, 2004;
10. RESNYANSKY Lucy, „*The role of technoloy în intelligence practice: linking the developer and the user perspectives*”, Prometheus, Sydney, 2010;
11. TRAN, Vasile, „*Teoria Comunicării”,* Bucureşti, Editura comunicare.ro, 2002.
12. WEIMANN, Gabriel, *www.terror.net: „How Modern Terrorism Uses the Internet”*, United States Institute of Peace, March 2004. http://www.usip.org/pubs/specialreports/sr116.html accessed on 15 March 2015.

MONITORING AND CONTROLLING INFORMATION SYSTEMS IN ORDER TO PREVENT IMPROPER USAGE AND ATTACKS FROM INSIDE THE ORGANIZATION

Dan FOSTEA
Major Engineer, Scientific Researcher III and PhD candidate, works within the Military Equipment and Technologies Research Agency, Bucharest, Romania,
e-mail: dfostea@acttm.ro

Ştefan-Ciprian ARSENI
Lieutenant. Engineer, Assistant Researcher and PhD candidate, works within the Military Equipment and Technologies Research Agency, Bucharest, Romania, e-mail: sarseni@acttm.ro

Bebe-Răducu IONAŞCU
Captain Engineer Scientific Researcher III, works within the Military Equipments and Technologies Research Agency, Bucharest, Romania, e-mail: bionascu@acttm.ro

Abstract: *Over the past decades, information has proven its vital role both in civilian and military organizations. Following the rapid development of information technology, armed forces have been developing integrated computer networks over different military structures, starting at battalion level. In general, these networks are secured through physical separation from outer attacks, but there still exists the possibility of an inner attack, no matter whether or not it is intentional. In order to reduce these risks or to strictly monitor the networks, several software solutions, that are transparent for the user, while assuring network integrity, can be applied. In this consideration, the monitoring of an information system can be achieved by integrating and interrogating certain parameters from inside that system, allowing the signaling of any software modifications. Also, for controlling any type of transfer using removable devices, a software solution can be implemented, so the risk of a possible security breach can be minimized.*

Keywords: *information security, network security, computer monitoring, transfer control*

Introduction

Widely known to the general public and to the military in particular, is the issue of securing information transfers between a network, military or otherwise, and external users or between different networks. Keeping the description at military level we are talking about changing information between own forces or with our allies. While this is still a key requirement for achieving a secure and reliable inter-connection of people and their devices, another security issue became a trend in the last years: insider threats.

Mainly concerned on outside attacks from hackers or cyber-terrorists or even military adversaries, organizations have directed their attention in securing only this area of risks, and did not pay much attention to the possible security breaches that could arise from inside the organization, probably caused by revolted employees. Yet, this type of inside threats could have a greater impact and cause damage on a bigger scale, while being harder to detect, than a regular type of outside attack.

To overcome these situations, security administrators can implement different security policies that will restrict and try to control the area of access of a regular user. Even so, a too strict security policy tends to severely reduce the advantages of using computers and not in the last place it is annoying the user. Keeping this in mind, there is still the problem regarding privileged users, who are not obligated to support these rigorous policies. To solve those problems there can be developed specialized applications to monitor the user activity and to control the means of transferring the information in or out the system.

1. Analyzing the problem

As described in "An Introduction to Computer Security: The NIST Handbook", NIST (National Institute of Standards and Technology) mentions eight major elements that a general security approach should be based on. Among those eight elements, the following ones can be considered a top priority when designing and implementing a security architecture inside a military organization:

- The organization's mission should be supported by the implemented security measures/policies;
- The management element should see security as an integral element of the organization;
- Security policies should consider the constraints imposed by societal factors, therefore it should be periodically reassessed;
- In order to assure an increased confidence in the organization's security procedures, they should be approached in a comprehensive and integrated manner.

As military personnel, we have to consider the problem of breaching the network, the integrated communications and information system, from the operational point of view. These being said, the same apply for any network essential for the functional and the operational capabilities of a certain entity.

Nowadays a command post from battalion up it is very crowded, not only with equipments but with many persons (Figure 1).

Figure no. 1. Marine corps base camp Lejeune [1]

The problem is controlling all these people while, in the same time, having a high level, efficient command. As a requirement for a perfect collaboration between nations, one's network has to interconnect to allied networks, therefore multiplying the risks of a possible threat that could inflict various types of damages and result in significant losses. Thanks to

[1]Marine corps base camp LEJEUNE, N.C. - Marines of 2nd Intelligence Battalion (photo by Lance Cpl. Joshua Brown), in http://www.iimef.marines.mil/Photos/tabid/131/igphoto/2000709438/Default.aspx, accessed on 28.03.2015

continuous improvements in securing outside interactions with a network, the risk of mitigating errors from "infected" computers located in outer networks has diminished.

Similar to outside attacks, inner threats can be traced under the form of fraud or data theft, employee sabotage or malicious software inserted in the network by employees. Since insiders are familiar with the system and have, in worst case scenario, unrestricted access to it, authorized users find themselves in the a better position to commit crimes. While, even in a minimum secured network, users need certain privileges to execute an action on the system, their entire activity is not totally constrained, therefore it does not matter if they are regular users or technical staff members, all of them can pose a threat.

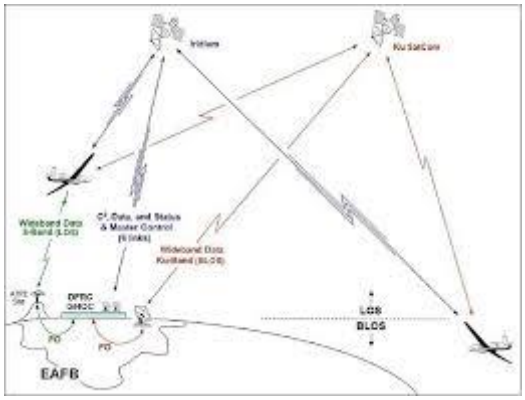


Figure no. 2. The Global Hawk communications arhitecture [2]

When talking about very complex communications and information systems, see for example Figure 2, all the above-described problems add up and form a difficult to counteract situation. The global HAWK system for communications is a very vivid example because its interactions are not only between users of the inner network controlling the flight, but also with its beneficiaries, the parties which are accessing the information, and the sensors themselves which are operating as remote connections to the network[2].

2. Identifying solutions

As stated in chapter 2, inner attacks can have many forms and induce different amounts of damage, when successful. In order to counter-attack these threats or, also, try to predict them, security administrators need to implement various policies or measures that can both limit and direct user's activities during his logon session.

One possible method of overcoming the challenges imposed by assuring a secure environment and protection from inside threats is the deployment of a system monitoring solution. It allows security administrators and employers to have a better insight of the activities employees are involved during work-time, in order to enable early detection of a threat before any damage is done to the organization. Also, based on the detailed insights, received under the form of daily, weekly or monthly reports, of insider activities and user behaviors, a rapid action and incident response can be conceived.

Depending on the level of access a user has, actively monitoring that user's activity will ensure that there are no unauthorized transactions taking place from that account or computer. By recording all high risk insider activities, as indicators of possible threats, an

[2] Global Hawk UAS (Unmanned Aerial System) of NASA, in https://directory.eoportal.org/web/eoportal/airborne-sensors/global-hawk, accessed on 28.03.2015

effective and practical security strategy, for protecting against elevated privileges ill-intended users, can be deployed.

Chapter 4 describes, from a technical point of view, a possible implementation of a user activity monitoring solution that administrators can use to actively or passively identify users prone to malicious activities or computers that might have been infected.

Most companies have implemented security systems and measures that can prevent external attacks such as antivirus, firewall, intrusion detection systems, but only few measures that take into account the threats coming from the ordinary employee who can remove confidential information out from the company for personal benefit or in other company benefit, or lose it by accident.

Without compromising the benefits of portable devices (portability), security of a transfer can be achieved primarily by making the data on a compromised device inaccessible to unauthorized users and processes, such as may be executed by malware. One common approach is the encryption of data for storage, and scanning the devices for malware with an antivirus program, although other methods are still possible.

Chapter 5 describes the risks of portable storage devices usage in an organization and presents the principal solutions to mitigate those risks.

3. Monitoring an information system

Taking into consideration the methods used to implement a system monitoring architecture, we can state that there are three possible means of implementation:

- *Passive monitoring* – systems are monitored only at specific time intervals or on certain moments when it is considered that a breach could have occurred;
- *Active monitoring* – systems are monitored for their entire period of functioning and any user activity is either being logged locally or transmitted over the network towards a command center;
- *Mixed monitoring* (network passive + local active) – systems are monitored locally in an actively manner, by logging any user or software activity, issuing an alert whenever a certain threshold is overcame. Yet, an administrator, located in a command center, can issue system state interrogation at any moment (this is considered to be the passive component).

3.1. Passive monitoring

A passive system monitoring solution is an application that mainly allows security administrators to create snapshots of a system, in certain moments, and then compare them, revealing any modification or data alteration that could have occurred in the time interval between those two snapshots. Regarding the operational flow when using this type of applications, the following stages can be viewed as a foundation for creating specific operational procedures, according to each security issue that is addressed:

- *Identification* – identify the system to be investigated;
- *Data acquisition* – creating a snapshot of the "clean" system, to preserve data;
- *Data Analysis and/or Data recovery* – in case the system is considered breached, a new snapshot will be taken. It will then be compared with the initial snapshot and any data alteration will be revealed. After this moment, if data has been lost, it could be restored using the "clean" snapshot.
- *Report* – depending on information gathered from the data analysis stage, specific reports can be created, presented and used as components for any future snapshot analysis.

Considering the functionalities that a passive monitoring solution could provide, it can also be used in performance analysis. Taken at regular intervals, snapshots could be used for observing resource usage trends or foreseeing potential software or hardware problems.

3.2. Active monitoring

Unlike passive monitoring, the active monitoring of an information system requires less interaction between the security administrator and the targeted system. Also, it allows a continuous monitoring of user or software activity on a targeted system, by implementing and agent-based infrastructure. These agents consist of applications that can produce results based on previous activity history or defined patterns, raising an alert each time a possible threat is identified. These alerts are concentrated in a command center, from which the administrator can act according to specific security procedures.

Starting from an agent-based infrastructure, an active monitoring solution can be composed of:

- Agents that filter data, but do not modify data flows in the system. In this case, an attacker could do a certain amount of damage that could also create a ripple in the entire network, if the alert is not raised as soon as possible.
- Agents that filter data and could modify data flows in the system. In this case, agents manage information inside the system and when an attack takes place, it not only raised an alert, but it also allows the administrator to undo any damage that the attacker might have inflicted to the system. The restoration can be possible because the agent it logging any modification both to the location of a file, but also to its content.

3.3. Mixed monitoring

Mixed monitoring combines the functionalities of both passive and active monitoring, by implementing an agent-based infrastructure, controlled from a central point. The main difference between active and mixed monitoring is that, in mixed monitoring, the security administrator could interrogate an agent at any time, pulling any type of information from the targeted system, not just only waiting for the agent to signal when an attack is in progress.

This method of integration provides also the possibility of monitoring a system's performance, allowing administrators to change security policies that could interfere with user's activities, leading to negative performances.

For active and mixed monitoring solutions, new filtering algorithms for agents have been developed, even some that are based on the notion of neural networks, that can assure a better detection rate and also adapt in case of newer type of attacks.

4. Controlling transfers

According to recent studies, a growing number of portable devices are used in organizations. Some examples are: notebooks, laptops, USB flash drives, advanced mobile phones and other mobile devices.

USB flash drives, for example, are the best choice for people who move files between computers and almost every user has at least one USB flash drive. Flash drives are small, thus they could easily get lost and the same happens with the data stored on it.

USB flash drives can pose two major challenges to information system security: data leakage and system compromise through infection with computer virus and other malicious software.

Data leakage

Data leakage is a growing phenomenon caused primarily by employees who have access to sensitive information through a growing list of devices, capable of multiplying and storing digital data, such as USB flash, mobile phones, and even digital cameras.

USB flash drives have large storage capacity relative to their low cost and small size, meaning that using them for data storage without adequate security measures can pose a serious threat to information confidentiality, availability and integrity. To reduce the risk of security breaches, secure USB drives should take into consideration the small dimensions and different form. :

- *Storage*: USB flash drives can be stored in bags, backpacks, laptop cases, jackets or pockets, or left at unattended workstations, being hard to track physically.
- *Usage*: a significant challenge is tracking sensitive data stored on personal flash drives which are small and constantly moving. While many companies have strict management policies toward portable storage devices, and some companies restrict all of them outright to minimize the risk, others seem unaware of the risks posed by these devices to system security.

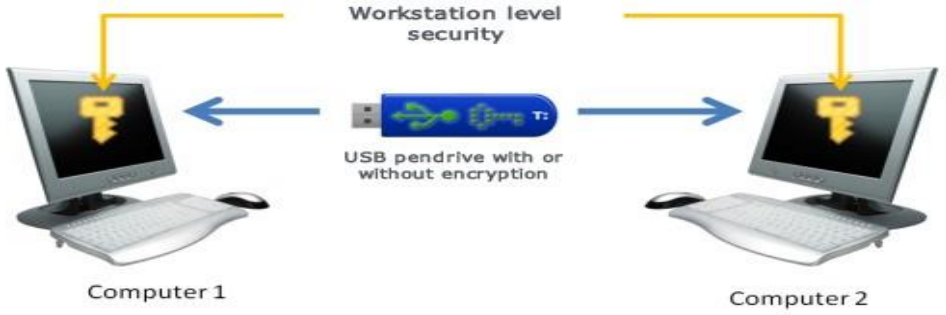
Malware infections

In the early days of computer viruses and malware the most important means of transmission and / or infection was the floppy disk. These days, USB flash drives perform the same role as the floppy disk, making USB flash drives a leading form of system infection. When a malware or a virus gets onto a USB flash drive it can infect all the devices into which is plugged in.

In 2011, a Microsoft study analyzing data from more than 600 million information systems in the world, documented the prevalence of virus and malware infection by means of removable USB flash devices. The conclusion of the study was that 26% of all virus and malware infections of Windows systems were due to exploiting the AutoRun feature in Microsoft Windows. Those findings were in line with other statistics made by antivirus company ESET, such as the monthly reporting of most commonly detected malware, which lists abuse of autorun.inf as first among the top ten threats in 2011.

The Windows *autorun.inf* file usually contains information on programs to run automatically when removable devices (often USB flash or similar devices) are accessed by a workstation user. The default setting for Autorun in Windows versions prior to Windows 7 will automatically execute a program listed in the autorun.inf file when someone accesses the removable device. Many types of malware make themselves copies onto removable storage devices. While this is not all the times the primary distribution mechanism, malware authors often design additional infection techniques.

Solutions



Data transfer's security becomes vital and can be done both at the workstation level, by real-time monitoring of physical ports and by controlling (restricting or approving) the transfer of documents using removable media, and at the device level by encrypting the content or restricting read/write rights.

Software encryption

Automatically and transparently encryption of the contents of a USB device can be done with software solutions such as dm-crypt, FreeOTFE, Data Protecto and TrueCrypt. Windows 7 Enterprise and Ultimate Editions, Windows 8 and 8.1 and Windows Servers 2008, 2012 provide a solution to USB drive encryption using BitLocker. The Apple Computer Mac OS X operating system has provided software for disc data encryption since Mac OS X Panther was issued in 2003[3].

In order to prevent access to files in case the drive becomes lost or stolen, additional software can be installed on an external USB device.

Hardware encryption

Some manufacturers design hardware encrypted USB devices with microchips providing automatic and transparent encryption. Some of this kind of devices requires a pin code entered into a physical keypad on the device for granting access to the content[4].

Physical ports monitor

Installing security software applications on company workstations may help track and minimize the risks of infections and data leaks.

Such security software application can monitor in real time all the events of physical ports and, using whitelists or blacklists, can approve or reject the external devices inserted in the system, according to security policies of the company regarding the sensitive information and security clearances for personnel handling the information.

[3] "How to create a password-protected (encrypted) disk image in Mac OS X 10.3 or later", in https://support.apple.com/en-us/HT201599, accessed on 26.03.2015

[4] "Toshiba Announces Encrypted USB Flash Drive", in http://www.toshiba.com/us/press-release/101244, accessed on 26.03.2015

Conclusions

There are different ways to protect ones data but the key is to do this in such a manner that we can still benefit from the advantages of the modern technology.

Monitoring and controlling are very important activities, but it is also important not to forget the goal of introducing the use of computers in military and the goal is same as in civilian life, to make our lives easier.

BIBLIOGRAPHY:

1. D. Dasgupta, F. Gonzalez, K. Yallapu, J. Gomez, R. Yarramsettii, "CIDS: An agent-based intrusion detection system", Computers & Security, Elsevier, 2005
2. N. Kussul, S. Skakun, "Neural network approach for user activity monitoring in computer networks", Proceedings of the 2004 Joint Conference on Neural Networks, 2004
3. T.F. Lunt, "Detecting Intruders in Computer Systems", Proceedings of Auditing and Computer Technology Conference, 1993
4. V. Paxson, "Bro: A System for Detecting Network Intruders in Real-Time", Proceeding of the 7th USENIX Security Symposium, 1998
5. D. Spinellis, "User-level operating system transactions", Software: Practice & Experience, Wiley, 2009
6. Eset Global Threat Report, December 2011
7. "Secure USB flash drives", European Union Agency for Network and Information Security, 1 June 2008, ISBN 978-92-9204-011-6
8. Microsoft Security Intelligence Report Volume 11, January-June, 2011
9. "An Introduction to Computer Security: The NIST Handbook", Special publication 800-12, NIST, 1995

AFFECTIVE COMPUTING – A COMPONENT OF WEB 3.0

Cosmin Dragos DUGAN
PhD candidate at "MIHAI VITEAZUL" National Intelligence Academy Bucharest, Romania,
e-mail: dugcosmin@yahoo.com

Abstract: *Affective computing features will be a defining attribute of Web 3.0, alongside intensification and diversification of the ways in which a user can interact via the Internet. The cyber-affective component will allow a concentration of content which is focused on the needs and desires of consumers, thus facilitating the modification of the emotional content in order to alter the perception and representation of the cognitive content in real time. For intelligence organizations affective computing is an additional (and complementary) dimension which is useful in the process of collecting information and obtaining access to a global audience. The possibility of modifying the emotional envelope attached to a cognitive content offers new degrees of freedom in influence operations that are a component of the fifth generation conflict (the neocortical war). This paper aims at presenting and detailing the concept of affective computing, its (current and prospective) main working instruments as well as potential applications within the following relevant to the intelligence sector fields: OSINT, online biometric identification, resilience and social engineering.*

Keywords: *affective computing, biometrics, OSINT, neocortical warfare, propaganda, social engineering*

Introduction

Access to information has become increasingly easier in contemporary society, thanks to the development and use of technologies of mass communication and data transfer. However, access to information did not automatically result in the obtaining of a high degree of knowledge and did not lead to the using of information for constructive or at least peaceful purposes only[1]. After the initial excitement, amid the first decade of the post-bipolar era, the Internet has become an important and later on indispensable component of the general activity carried out by any increasingly connected to the globalist phenomenon individual. Almost no human activity lacks a corresponding Internet content, whereas the behavior of users is also the main causal factor that is responsible for the latter's inputs, changes and evolution. The Internet is considered to be a more permissive expression environment, that is easily accessible, and that provides access to a potential global audience. As such, the Internet has become the ideal channel for communicators and for propagation of messages – ranging from more or less beningn advertising spots, to humanitarian campaigns, news or political ideologies. Although both the size and the social impact of communication via the Internet had been initially recognized, further analyses of events that have happened during the last quarter of the century have shown the degree to which the affective dimension resulting from joining of a global audience had been actually underestimated.

The emergence and development of social networks allowed for the study of the emotional dimension of communication within selected groups of Internet users, a fact that facilitated the development of new techniques of commercial and political marketing that are widely used today. As the largest global trading hub, the Internet has proven equally effective

[1] Irena Chiru-Dumitru, *Gândire critică pentru intelligence în era informaţională*, Sesiunea de Comunicări ANI, Bucureşti, 2012.

in distributing malignant propagandistic and ideological messages, which led to the emergence and development of a seris of phenomena such as online self-radicalization and radicalization that are now commonly used as resources for Islamic-inspired terrorism[2]. The many ways by which Internet might affect national security or by which elements of national security have become increasingly dependent on the use of the online environment have generated the need to develop specialized tools for the monitoring, collection and processing of information in the online environment as well as tools for cyber security.

As such, the increasingly extended access to real-time information that is obtained from open sources (OSINT - open source intelligence) has generated a true "OSINT revolution" with impact on intelligence and national security policies. Continuous development of services offered to users via the Internet, of human-computer interaction modalities and the increasing global connectivity and current dynamic of the security environment resulted in having the OSINT products centered around concepts such as alert, and early and strategic warning.

2. Affective computing - the next stage of the analysis of the feelings expressed in the online environment

The analysis of user generated content (user activities that are stored by providers – such as accessed sites, Internet purchases, blog or social networks comments) has grown stronger over the past decade, (in ideal cases) allowing for the identification of anonymous users, as well as for the analysis of intentions and of the degree of risk to national security. Although there are a number of difficulties, such as the large amount of unstructured data gathered from multiple sources that require automatic processing, the difficulty of contextualization, and the automatic multichannel data fusion, the field is in the process of accelerated development.

In particular, we intend to refer to those techniques that are involved in the identification and modeling of individual and collective emotional behavior, starting from the analysis of user-generated content. Currently, the most widely used technique is the semantic analysis of online content (especially "sentiment analysis" – sentiment analysis and opinion mining) that performs automatic analyses of natural language in order to identify and extract subjective information from within the analyzed materials. The result is the identification of the author's affective state upon drafting the text (that is expressed under the form of emotions, attitudes or opinions) and of the emotional intensity and the type of emotions that the author wishes to share with the audience.

The limitations of the method are nevertheless evident – the accessing of emotions by using one channel only (that of the written language), the possibility of fraud on behalf of the source, translation and adaptation difficulties of multilingual or multicultural texts, contextualization difficulties, etc. In fact, it is these limitations that have stimulated research of additional ways to identify affective status of a source of interest.

A related area of interest, which is also based on user-generated data processing, is the one centered on online biometric identification. Within the current paper we argue in favor of such a joint approach by also emphasizing the fact that the more complex the results of the analyses become, the easier it is to develop (affective and cognitive) behavior patterns that can be used to identify the source (online personality – affective cyberprofile). The joint approach provides better identification of the author’s or authors' intentions and risk evaluation.

[2] Cristian Barna, *Jihad în Europa – amenințarea teroristă de “franciză Al-Quaida”*, Intelligence Revue, march 2011, pp. 14-18, accessible online at adresa http://www.sri.ro/fisiere/ publicatii/intelligencemartie2011.pdf.

1. For a first step we approached the subject of diversification of those channels aimed at acquiring of unorganized data that can be used in order to determine the affective status of the source:

- *Verbal communication* allows for a psycholinguistic analysis of discourse and recognition of certain features of the spoken language, that enable the identification of the author. The text of verbal conversations that is generated as an automatic transcription by using of specialized software (e.g. software that is produced and sold by Sail Labs) is being analyzed in terms of semantics by means of particular tools that are pertaining to sentiment analysis. As such, the identification of passages of text that are strongly impregnated by emotions is envisaged, but also the recognition of tense and dramatic moments, that anticipate or require an intense emotional involvement on behalf of the audience[3] or, on the contrary, vague and allusive statements (that might be wrongly classified by a classical system of automatic analysis)[4]. In parallel, prosody is also being analyzed (the auditory-vocal dimension of verbal communication) – which provides information on the linguistic variability of high- or low-pitched voice (intonation), rhythm (including breaks) and the speed of speech, and hesitations (fluency) [5]. Specialized software than allows for the identification of certain features that are of interest to the beneficiary – identification of intentions (e.g. the imminence of a violent action, spreading of ideological messages), aspects of personality (potential psychotic disorder, PTSD, high-functioning autism, cognitive impairment, etc.) [6].

- *The non-verbal language* is referring to the identification and processing of images containing data about expressions and attitudes that convey a (detectable and quantifiable) emotional state, as well as of the way they are set forth and their temporal evolution (frequency, duration, time of onset).

Its importance is generated by the fact that, on average, the proportion by which affective and attitudinal contents are conveyed by nonverbal means amounts to 55%, whereas paraverbal and verbal transmiters add up to 38% and only 7% respectively. As such a verbal message that is not accompanied by its nonverbal and paraverbal components will be harder to decode. The systematic study of the gestural facts falls under the kinetics' area of interest, that breaks down behavioral signs to the smallest action units of gesture or mimic (kinema), that are to be later on analyzed and integrated within a psychological, social and cultural context.

The field of research is extremely broad and requires a different approach.

- Facial expressions can be recognized by means of specialized software, that allow for the putting together of an individualized library of expressions and affective occurences, starting from images or video captions (social networks) [7]. The combined analysis of facial expressions and eye movements with that of the language is of particular interest, given the cultural influences that have the tendency to encode the discourse, in contrast with the quasi-

---

[3] Brian O'Neel, , Mark Riedl, *Toward a Computational Framework of Suspense and Dramatic Arc*, pp. 246-256, in Sydney D'Mello, Arthur Graesser, Bjorn Schuller, *Affective Computing and Intelligent Interaction,* 4th International Conference, ACII 2011, oct. 2011, Ed. Springer-Verlag, SUA, 2011.

[4] Jeroen Dral, Dirk Heylen, Rieks op den Akker, *Detecting Uncertainty in Spoken Dialogues: An Exploratory Research for the Automatic Detection of Speaker Uncertainty by Using Prosodic Markers, in* Khurshid Ahmad (editor), *Affective Computing and Sentiment Analysis Emotion, Metaphor and Terminology,* Ed. Springer-Verlag, SUA, 2011.

[5] Thurid Vogt, Elisabeth Andre, Johannes Wagner, Automatic *Recognition of Emotions from Speech: A Review of the Literature and Recommendations for Practical Realisation,* pp. 74-92, in Russel Beale, Christian Peter, *Affect and Emotion in Human-Computer Interaction, From Theory to Application*, Ed. Springer-Verlag, SUA, 2008.

[6] Demetrios Sapounas, Vadim Kagan , Edward Rossini, *Sentiment Analysis for PTSD Signals,* Ed. Springer-Verlag, SUA, 2013, pag. 9, 30-32.

[7] Jiebo Luo, Quanzeng You, Hailin Jin, Jianchao Yang, *Robust Image Sentiment Analysis Using Progressively Trained and Domain Transferred Deep Networks*, 29th AAAI Conference on Artificial Intelligence in Austin, Texas, ian. 25-30/2015 , accesibil online la adresa http://www.cs.rochester.edu/u/qyou/papers/sentiment_analysis_final.pdf.

universality of affective facial expressions[8].

- Eye movements and pupillometry is an extensively studied field, that allows both for the assessment of emotional status as well as for the highlighting of certain physiological and pathological features. Changes in size, equality or pupillary reactivity in different circumstances (that are either under control or can be evaluated) allow for an extremely accurate assessment of emotional status, as ocular reactions are involuntary and have a high degree of expressiveness. In clinical practice there are electronic pupillometers that can perform an entire battery of tests in order to assess spontaneous or provoked pupil reactivity. The tests can be adapted to the means by which image is acquired (video sources) and to the purpose[9].

- Variations of posture, attitude and gestures can be identified by using video files that can be later on interpreted by means of dedicated software. By using even small sets of data, information on the personality type of the source can be obtained[10], whereas the using of serial recordings facilitates high quality assessments. For example, computer processing of video images of Hitler (especially during his speeches) led to the conclusion that toward the end of his life he might have suffered of the Parkinson disease[11]. A multidimensional analysis that was conducted in 2008, which also included a component on automatic analysis of gestures, concluded that Vladimir Putin might suffer from an autistic type neurodevelopmental disorder (Asperger syndrome)[12].

- Music, rhythmic sounds and auditory alerts can have a major impact on the audience's emotional state (the psychoacoustic component). For example, video recordings made by jihadist groups often have a musical background which is in conjunction with the message, in order to increase its affective impact, while also representing a powerful symbol of cultural identity (emotional optimization)[13].

- *Biosignals* are signals pertaining to the electromagnetic spectrum (electric, magnetic, thermal) that are emitted by the human body as a result of the electrochemical activity of the cells. Biosignals are subject to detectable changes according to the condition of the studied individual (state of health or disease, emotional status, neuroendocrine changes) and allow for a specific evaluation of the investigated biological systems.

Experiments are attempting to process data obtained by monitoring of heart and breathing rate, of uni- and multi-channel electrocardiogram, of electroencephalogram, of phonocardiogram, of electrical activity of the skin (electrodermal activity), of electromyogram at the level of certain muscles that are involved in the creation of facial expressions (orbicular of the mouth, rizorius, zygomatic), of discrete changes in facial temperature, etc. The benefit consists in the fact that all of the above are involuntary indicators of the emotional state, allowing for discrimination between natural and controlled reactions.

Biological signals obtained by means of ECG and EEG are the most commonly used

---

[8] Xiaozhou Wei, Johnny Loi, Lijun Yin, *Classifying Facial Expressions Based on Topo-Feature Representation,* pp. 69-83, in Jimmy Or, *Affective Computing Focus on Emotion Expression, Synthesis and Recognition*, Ed. I-TECH Education and Publishing, Vienna, 2008.

[9] Andrew Duchowski, *Eye Tracking Methodology Theory and Practice*, Ed. Springer-Verlag, SUA, 2007 .

[10] Markus Koppensteiner *Motion cues that make an impression: Predicting perceived personality by minimal motion information* , Journal of Experimental Social Psychology Volume 49, Issue 6, November 2013, pp. 1137–1143 accessible online at http://www.sciencedirect.com/ science/article/pii/S0022103113001467.

[11] Neil Midgley, *New technology catches Hitler off guard, The Telegraph*, 22 nov 2006, accessible online at http://www.telegraph.co.uk/news/uknews/1534830/New-technology-catches-Hitler-off-guard.html

[12] Brenda Connors, *A Technical Report on the Nature of movement pattening*, the brain and decision-making, 2008, accessible online at http://www.naegele.com/documents/200report.pdf.

[13] Ana Tajadura-Jiménez, Daniel Västfjäll, *Auditory-Induced Emotion: A Neglected Channel for Communication in Human-Computer Interaction*, pp. 61 - 71 in Christian Peter, Russel Beale, *Affect and Emotion in Human-Computer Interaction*, Ed. Springer-Verlag, SUA, 2008.

and have a high specificity. In recent years ("dry" or even touchless), noninvasive means that catch the signal have been developed which simplify to a great extent the process of acquiring data. In particular, brain-computer interfaces have been significantly enhanced, with increased interest in the further development of this field[14].

At first, the acquisition of biological signals had been performed by way of experiments under controlled conditions. Subsequently it has been applied in neuromarketing or political marketing studies. Consistent results depend on optimal acquisition of signals for a relatively long period of time, on the possibility of establishing a basic level, and on the knowledge of context that allows for removal of artifacts and insignificant reactions. The acquisition process of real-time and from a distance biosignals from an anonymous target that adopts a covert behavior of its activity on the Internet is still difficult, but not impossible. As such, bio-signs can be acquired by devices used in neuro-games (games using bio-feedback or affective feedback – emotionally responsive computer games), immersive games or wearable technologies used to monitor physiological parameters (extensions of mobile phones, watches or intelligent bracelets, electronic tattoos, implantable microprocessors – in short, a continuosly growing and diversifying market)[15]. A series of bioelectrical signals can be extrapolated or indirectly acquired[16].

- *Relational data* refer to the online relational environment derived from accesing of social networks or with which the target voluntarily interacts by using a communication channel (with affective valence). Specific processing of these pieces of data provides information that helps to shape the emotional profile – for example aspects of personality, personal preferences, sympathies / antipathies[17], sexual orientation[18], use of recreational or narcotic substances, etc. Computational sociology of affective states (Computational Affective Sociology[19]), as a specialized subdomain, aims to develop tools that are able to extract relevant information about the emotional profile of an individual as part of a group and on how an individual can affect the emotional status of a social network.

- Biometric data may be obtained by using one or more communication channels via the Internet. In general it refers to anatomical, physiological or behavioral elements that are very difficult to duplicate or forge and that can be obtained by processing of the acquired data[20].

- Fingerprints can be reproduced from high-resolution photos that allow for generating of a complete image of the fingerprint followed by its duplication[21]. Recently, a German hacker – Jan Krissler ("Starbug") has used this technique to obtain a fingerprint of German

---

[14] Christian Muhl, Egon L. van den Broek, Anne-Marie Brouwer, *Multi-modal Affect Induction for Affective Brain-Computer Interfaces*, pp. 235-245, in Sidney D'Mello, Arthur Graesser et all, *Affective Computing and Intelligent Interaction*, Ed. Springer-Verlag, SUA, 2011.

[15] William Sims Bainbridge, *Computational Affective Sociology*, pp. 23-35 in Russel Beale, Christian Peter, *Affect and Emotion in Human-Computer Interaction*, Ed. Springer-Verlag, SUA, 2008.

[16] Didem Gökçay, Gülsen Yildirim, *Affective Computing and Interaction: Psychological, Cognitive and Neuroscientific Perspectives*, pp. 310-315, IGI Global, SUA, 2011.

[17] *Top-Secret Document Reveals NSA Spied On Porn Habits As Part Of Plan To Discredit 'Radicalizers'*, The Huffington Post, 11.26.1013, accessible online at http://www.huffingtonpost.com/2013/11/26/nsa-porn-muslims_n_4346128.html.

[18] Carter Jernigan, Behram Mistree, *Gaydar: facebook friends expose sexual orientation*, First Monday, vol. 14, nr. 10, oct. 2009.

[19] For supplementary information please access the following site – Association for the development of affective computing at http://emotion-research.net/.

[20] Omar Alzoubi, Md. Sazzad Hussain, Sidney D'Mello, Rafael A. Calvo**,** *Affective Modeling from Multichannel Physiology: Analysis of Day Differences*, pp. 4-14, in Sidney D'Mello, Arthur Graesser et all, *Affective Computing and Intelligent Interaction*, Ed. Springer-Verlag, SUA, 2011.

[21] Geppy Parziale, *Touchless Fingerprinting Technology*, pp. 31-38, in N.K. Ratha, Venu Govindaraju, *Advances in Biometrics*, *Sensors, Algorithms and Systems,* Ed. Springer-Verlag, SUA, 2011.

Defence Minister - Ursula von der Layden[22].

- Vascular (palmar, facial, retina) drawing can be obtained by using specialized software or by means of special exposure cameras[23].

- The aspect of the iris –high resolution images are required[24].

- Voice recognition is an intensively researched field, which allows for in-depth analysis of the human voice.

- The dynamics of the lips (the pronunciation of sounds, words, some facial expressions as well as smiles, laughter and disgust) – multiple serial images are required.

- Bioelectrical signals (ECG, EEG) – are hard to forge, but may undergo significant changes depending on a number of physiological or pathological conditions. However, if monitored for a sufficient period of time, the results are excellent.

- Behaviors resulting from human-computer interaction (behavioral recognition) are a byproduct of the use of the online environment. Yet, they constitute a behavioral pattern that is sufficiently specific and hard to counterfeit. A series of generally involuntary behaviors are generated by direct interaction with computers – the typing rhythm (keystroke dynamics), the pressure used when using a liquid crystal screen, the manner in which the mouse is being handled (mouse dynamics)[25]. The most common patterns of behavior refer to the use of electronic mail, electronic data storage, and the strategy used in some games (strategy, MMORPGs, FPS, driving) etc. For example, the analysis of the contribution of a participant in a game can be useful in generating a statistical model of its skills and its possible professional areas[26] or in determining the role that it assumes within a hierarchy[27]. Also in recent years short-term memory has been explored as a behavioral marker, which could be extrapolated from mouse movements within situations that involve solving complex activities[28]. The improvement of behavioral recognition patterns allowed for the development of security solutions based on these biometric methods[29].

The best results are obtained by simultaneous use of several methods that characterize the target by using multiple channels independently acquired and processed data[30]. This data fusion facilitates the assemblying of a huge number of combinations between the various employed methods, providing for individual solutions that depend on the particularities of the

---

[22] Alex Hern, *„Hacker fakes German minister's fingerprints using photos of her hands",* accesibil online la adresa http://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands.

[23] Masaki Watanabe, *Palm Vein Authentication*, pp. 8-14, in N.K. Ratha, Venu Govindaraju, *Advances in Biometrics*, *Sensors, Algorithms and Systems,* Ed. Springer-Verlag, SUA, 2011.

[24] James R. Matey, David Ackerman, James Bergen, Michael Tinker, *Iris Recognition in less Constrained Enviroments*, pp. 110-117, in N.K. Ratha, Venu Govindaraju, *Advances in Biometrics*, *Sensors, Algorithms and Systems,* SUA, Ed. Springer-Verlag, 2011.

[25] Kenneth Revett, *Behavioral biometrics. A remote controll acces*, Editura Wiley, SUA, 2008, pp. 73-96.

[26] Gang Wang, Andrew Gallagher, Jiebo Luo, David Forsyth, *Recognizing Occupations Through Probabilistic Models: A Social View,* pp. 117-133, in Ming Shao, Yun Fu, *Human-Centered Social Media Analytics*, Ed. Springer-Verlag, SUA, 2014.

[27] Benedikt Fuchs, Didier Sornette, Stefan Thurner, *How Virtual Gaming Worlds Are Revealing the Nature of Human Hierarchies Emerging Technology*, in arXiv, 19.03.2014 accessible online at http://www.technologyreview.com /view/525696/how-virtual-gaming-worlds-are-revealing-the-nature-of-human-hierarchies/?utm_campaign=socialsync&utm _medium=social-post&utm _source=facebook.

[28] Roman V. Yampolskiy, *Behavioral, Cognitive and Virtual Biometrics*, pp. 355-368, in Albert Ali Salah, *Computer Analysis of Human Behavior*, Ed. Springer-Verlag, SUA, 2011.

[29] Chorng-Shiuh Koong, Tzu-I Yang, and Chien-Chao Tseng, *A User Authentication Scheme Using Physiological and Behavioral Biometrics for Multitouch Devices,* The Scientific World Journal, Volume 2014 (2014), Article ID 781234, accessible online at http://www.hindawi.com/journals/tswj/2014/781234/.

[30] University of Calgary, *"Researchers advance biometric security"*, ScienceDaily, 21 june 2012, accessible online at http://ucalgary.ca/news/utoday/june19-2012/biometric.

objective and of the available acquisition channels[31].

There are several ways by which a source can minimize its online biometric trace[32], including the altering or masking of its physionomy. For example, advanced versions of the ordinary masks are the anti-supervising masks[33] or holographic facial projections[34].

2. **(**One- / Multi-channel**)** *affective modeling* – comprises two fields of activity: on the one hand, *affective simulation*, that is responsible for the emulation of affective reactions that are compatible with those specific to humans, which is used in social robotics (humanoid robots or autonomous agents that interact with the public) and, on the other hand, *affective decoding*, whose aim is the automatic identification of human emotions by means of processing of a uni- / multi- channel signal that is emitted by a source. Decoding of emotional states can be either achieved by using the signals provided by a single channel (voice analysis, pupillometry, automatic analysis of facial expressions, etc.) or by merging processed data coming from two or more channels[35]. By pursuing this association, the degree to which emotions are identified can amount to 80-90% (two channels) or to 90% (three channels), as compared with a much lower rate of merely 30-60% when information coming from one single emotional communication channel is used[36]. The result of the affective modeling process is conveyed under the form of an avatar of the subject (artificial affective profile), which nevertheless represents but a course and time-limited model of the affective profile of the source, in other words a potential facet of its personality[37].

3. *Contextualization of data and online and real personality emulation* involves the development of a comprehensive psychological profile, by using all pieces of (cognitive, affective, biometric, and relational) information that can be obtained about the target via the Internet. Several personality traits are taken into consideration (the way in which the subject is relating itself to the social and cultural norms or to the authority sources, its self-image and self-esteem, the components of its personal prestige, and cognitive and emotional intelligence assessment), such as behavioral patterns (with focus on the online ones like habits, compulsive and stereotyped behaviors or attitudes to certain stimuli among which violent news with religious tones, and other stimuli-triggers), instinctual life (schedule of activity and rest, and food and sexual appetite), skills and abilities (training, areas of interest and excellence, technical and IT skills, interest in technology – is the subject interested in new technology or rather in conservative one?, etc). Special attention is given to the – virtual and real – relational environment and to the analysis of the cognitive and affective content of communication with various nods of the social network. An emerging area of interest in this direction is the processing of social signals (Social Signal Processing[38]), whose purpose is the decoding and the automatic synthesis of attitudes generated by non-verbal communication between socially connected actors. As a result, a hierarchy within the social network can be

---

[31] Md. Sazzad Hussain, *Hybrid Fusion Approach for Detecting Affects from Multichannel Physiology* in Sydney D'Mello, Arthur Graesser, Bjorn Schuller, *Affective Computing and Intelligent Interaction,* 4th International Conference, ACII 2011, oct. 2011, Ed. Springer-Verlag, SUA, 2011.

[32] Ann Cavoukian, Alex Stoianov, *Biometric Encryption: The New Breed of Untraceable Biometrics*, pp. 655-661, in Nikolaos V. Boulgouris (editor), *Biometrics Theory, Methods, and Applications*, Ed. Wiley, SUA, 2010.

[33] Please watch the video at http://www.urmesurveillance.com/urme-prosthetic/.

[34] Please watch the video at https://vimeo.com/103425574.

[35] Massimo Piccardi, Maja Pantic, *From the Lab to the Real World: Affect Recognition Using Multiple Cues and Modalities,* pp.196-213, in Jimmy Or (coord.), *Affective Computing Focus on Emotion Expression, Synthesis and Recognition Hatice*, I-Tech Education Publishing, SUA, 2008.

[36] Mincheol Whang, Joasang Lim, *A Physiological Approach to Affective Computing*, pp. 309-321, in Jimmy Or (coord.), *Affective Computing Focus on Emotion Expression, Synthesis and Recognition Hatice*, I-Tech Education Publishing, SUA, 2008.

[37] Marcin Skowron, Stefan Rank, *The Good, the Bad and the Neutral: Affective Profile in Dialog System-User Communication*, pp. 337-347, in *Affective Computing and Intelligent Interaction*, Ed. Springer-Verlag, SUA, 2011.

[38] For supplementary information please access the following site – european project SSPNET at http://sspnet.eu/.

established – either vertically, which covers impersonal relations such as power, prestige and leadership, or horizontally, that describes emotional closeness[39]. The identification of the degree of emotional contamination that a message can induce within a social network (as it is considered to mimic and automatically sincronize expressions, postures, attitudes, and gestures of another person, thus a state of emotional convergence being achieved) is also of particular importance. The ability to influence, polarize and produce affective convertion of the network elements is a potential indicator of the variation in importance and prestige of a certain network node, thus facilitating the propagation of messages[40]. The result of this process is a complex and multidimensional profile of the target, that facilitates the carrying out of an assessment about the intentions and risks posed to national security, as well as about potential behavioral reactions within certain scenarios[41].

4. *The analysis of intentions* refers to the evaluation of the level of risk according to which the target will commit acts that may affect national security – online radicalization or self-radicalization, cyber attacks, promoting of violent, racist or extremist doctrines or ideas, intentions to commit a terrorist or antisocial act, etc. Such a predictive-type assessment enables the drawing up of an anticipatory strategy meant to prevent and counteract these phenomena. A complementary strategy is the identification of those people who are at high risk of suffering an aggression via the Internet or demonstrate an increased vulnerability toward being recruited and radicalized. An example is the world premiere technology developed by the Fujitsu company, that is intended to identify people who have an increased susceptibility to suffer a cyber attack. Its working method consists in the drawing up of a psychological profile of employees (by electronic questionnaire) as well as of a profile of their online activity, additional elements that favor a reckless or negligent conduct at work thus being identified[42].

5. In some cases*, prevention strategies* can make use of virtual agents (emotional agents meant to change behavior – affective agents for behavior change), that are capable of automatically performing certain components of cognitive and affective analysis of the discourse. These agents have a high degree of artificial intelligence that allows them to automatically generate (by means of a predetermined algorithm) interactive counter-narratives (or interactive storytelling) in response to violent or violence-inciting narratives. The goal is the early detection of risk nodes within a social network, their automatic monitoring, isolation and diminishing of their ability to proliferate unwanted memes[43].

Conclusions

Affective computing elements will constitute a defining feature of Web 3.0, alongside the intensifying and diversification of the ways by which interaction with the user is pursued. The cyber-affective component will allow for a focusing of content on the needs and desires of the consumer, thus facilitating the transmission of the cognitive content via real-time

[39] Oya Aran, Daniel Gatica-Perez, *Analysis of Group Conversations: Modeling Social Verticality,* pp. 293-310, in Albert Ali Salah, *Computer Analysis of Human Behavior,* Ed. Springer-Verlag, SUA, 2011.

[40] Goncalo Pereira, JoanaDimas**,** *A Generic Emotional Contagios Computational Model*, pp. 256-267, in Sidney D'Mello, Arthur Graesser et all, *Affective Computing and Intelligent Interaction*, Ed. Springer-Verlag, SUA, 2011.

[41] Didem Gökçay, Gülsen Yildirim, *Affective Computing and Interaction: Psychological, Cognitive and Neuroscientific Perspectives*, IGI Global, SUA, 2011, pp. 425-435.

[42] *Fujitsu Develops Industry's First Technology That Identifies Users Vulnerable to Cyber Attack Based on Behavioral and Psychological Characteristics*, accessible online at http://www.fujitsu.com/global/about/resources/news/press-releases/2015/0119-01.html.

[43] Thurid Vogt, Elisabeth Andre, Johannes Wagner, *Automatic Recognition of Emotions from Speech: A Review of the Literature and Recommendations for Practical Realisation*, pp. 75-92, in William Sims Bainbridge, *Affect and Emotion in Human-Computer Interaction*, Ed. Springer-Verlag, SUA, 2008.

optimization of the affective content.
Nevertheless, the price that needs to be paid for these benefits is the sacrificing of private space. However, this concept will be difficult to conceptualize and quantify. The main goal is the ajustement of the "affective lens" through which a global audience will perceive reality and the manner in which the alteration of perception, representation and motivation of the cognitive content will interfere with the individual and collective decisional process.

For intelligence organizations the affective computing is an additional (and complementary) dimension aimed at collecting information and accessing of a global audience. The possibility to modify the affective envelope atached to a cognitive content offers new degrees of freedom in operations meant to influence public opinion, that are components of the fifth generation conflict (neocortical war). In addition to its being used for offensive purposes in the context of information warfare, there is also a protective dimension that is designed to amplify the degree of emotional resilience of the population, in case of conflict or natural or man-made disasters[44]. "Epidemics" of panic far outweigh the actual impact of localized events, that are amplified (often irresponsibly, but sometimes also in a directed manner) by the resonance box of the online environment. Another defensive valence is the use of virtual agents with artificial intelligence that are capable to automatically or in collaboration with a human supervisor generate counter-narratives that are affectively modulated according to the messages provided by the monitored source.

The ability to establish in real time the profile and the affective state of a certain target will determine, at least theoretically, a higher degree of safety (in transport and current social life), due to increased probability of detecting terrorist attacks, aggressive passengers or inadequate crew. It remains to be seen what is the limit beyond which these techniques will prove themselves detrimental as a result of their degree of instrusiveness that contribute to the dissolution of social masks – the border (still!) between the public space and the confort zone of emotional intimacy of individual thoughts and feelings.

BIBLIOGRAPHY:

1. Sydney D'Mello, Arthur Graesser, Bjorn Schuller, *Affective Computing and Intelligent Interaction,* 4th International Conference, ACII 2011, oct. 2011, SUA, Ed. Springer-Verlag, 2011.
2. Khurshid Ahmad (editor), *Affective Computing and Sentiment Analysis Emotion, Metaphor and Terminology,* SUA, Ed. Springer-Verlag, 2011.
3. Russel Beale, Christian Peter, *Affect and Emotion in Human-Computer Interaction, From Theory to Application*, SUA, Ed. Springer-Verlag, 2008.
4. Demetrios Sapounas, Vadim Kagan, Edward Rossini, *Sentiment Analysis for PTSD Signals,* SUA, Ed. Springer-Verlag, 2013.
5. Jimmy Or, *Affective Computing Focus on Emotion Expression, Synthesis and Recognition*, Ed. I-TECH Education and Publishing, Vienna, 2008.
6. Andrew Duchowski, *Eye Tracking Methodology Theory and Practice*, SUA, Ed. Springer-Verlag, 2007 .
7. Christian Peter, Russel Beale, *Affect and Emotion in Human-Computer Interaction*, SUA, Ed. Springer-Verlag, 2008.

[44] Sara B. King, *Military Social Influence in the Global Information Environment: A Civilian Primer*, Analyses of Social Issues and Public Policy, Vol.11, pp. 1–26, dec. 2011, accessible online at http://onlinelibrary.wiley.com/doi/10.1111/j.1530-2415.2010.01214.x/abstract; jsessionid=9D83E69CB59269B4FC11A8FEB318FCEB.f02t02.

8. Didem Gökçay, Gülsen Yildirim, *Affective Computing and Interaction: Psychological, Cognitive and Neuroscientific Perspectives*, SUA, IGI Global 2011.
9. N.K. Ratha, Venu Govindaraju, *Advances in Biometrics*, *Sensors, Algorithms and Systems,* SUA, Ed. Springer-Verlag, 2011.
10. Kenneth Revett, *Behavioral biometrics. A remote controll acces*, pp. 73-96, Editura Wiley, SUA, 2008.
11. Ming Shao, Yun Fu, *Human-Centered Social Media Analytics*, SUA, Ed. Springer-Verlag, 2014.
12. Albert Ali Salah, *Computer Analysis of Human Behavior*, SUA, Ed. Springer-Verlag, 2011.
13. Nikolaos V. Boulgouris (editor), *Biometrics Theory, Methods, and Applications*, SUA, Ed. Wiley, 2010.
14. Jimmy Or (coord.), *Affective Computing Focus on Emotion Expression, Synthesis and Recognition Hatice*, I-Tech Education Publishing, 2008.

THE FIGHT AGAINST TERRORISM – BETWEEN THE POLITICAL ACTION AND THE PROFESSIONAL ACTIVITY CHARLIE HEBDO, THE FREEDOM OF SPEECH AND THE NEW TERRORISM

Luminiţa Ludmila (CÎRNICI) ANICA
PhD candidate, "CAROL I" National Defence University, Bucharest, Romania,
e-mail: ludmila.anica@gmail.com

Abstract: *For the last two decades, terrorism was the most challenging topic of the Euro-Atlantic security. "Nine-eleven" showed that terrorist have no limits, and there are no safe areas for innocent people. The new terrorism was identified mainly with the violence promoted by some extremists pretending to be Al-Qaeda's Muslim believers. Last decade, we were confronted with a new sort of terrorism – rooted in Europe by local Al-Qaeda's followers. European homegrown terrorism took many lives of the innocent civilians in Madrid and London, and recently in France. The new phase of ISIS terrorism sent us a strong warning over the increasing risk.*

Fighting terrorism became a task of political power, of the security structures and, also, of the citizens. The article is intending to develop new ideas focused on the political action, aiming at preventing and combating terrorism through political, economic and social activities and by professional actions of security services.

Keywords: *Terrorism, terroristactions, thenewterrorism, Paris, Charlie Hebdo, Al-Qaeda*

Introduction - Theoretical considerations about terrorism

The word "terrorism" has an important political, socio-psychological and emotional load, underlining the difficulty of a precise definition. To define the terrorist phenomenon is, still, an essential issue for the success of its understanding as well as for the success of the prevention measures to counteract the same.

The Explanatory Dictionary of the Romanian language defines *terrorism* as *"the total amount of intentional violent acts of a group or of an organization in order to inflict a generalized fear and in order to reach some political purposes[1]"*. Considered as a French etymology, the word "*terrorism*" immerged from the European culture and the Latin language, where "*terrere*" means "*to tremble*", "*to frighten*" (or to be frightened)[2], and where from the word has been borrowed and processed to the forms still existing in use today, not only in the European languages but also in the whole world, the emotional meaning being that of "*horror, acute fright, powerful fear*".[3]

Terrorism is considered to be the main security risk during the recent years and the

[1]DEX, Dicţionarul Explicativ al limbii române (The Explanatory Dictionary of the Romanian Language), *Definiţia terorismului (Definition of terrorism),* available on-line at: http://www.dexonline.ro, accessed on February 14, 2015.
[2]http://www.arduph.ro/domenii/diu-si-terorismul/consideratii-generale-privind-terorismul/ online article, which cites John F. Kennedy's statements, 06 June 1962, available online, accessed on February 14, 2015.
[3]Atanasiu, Mirela; Repez, Filofteia: *Securitatea şi apărarea ţării în contextul ameninţărilor teroriste, (Security and national defence in the context of terrorist threats),* "Carol I" National Defence University Publishing House, Bucharest, 2013, page 21, available online, accessed on February 14, 2015: http://cssas.unap.ro/ro/pdf_studii/securitatea_si_apararea_tarii_in_contextul_amenintarilor_teroriste.pdf.

terrorist attacks targeted against some symbolic objects of western civilization and power prove the fact that international terrorism, structured in trans-frontier networks, represent the most serious menace to the life and freedom of the human beings, to democracy and to the other fundamental values sustaining the democratic community of the Euro-Atlantic States[4].

The international terrorist networks have access to up-dated technology and are able to use bank transfers and rapid communication systems, infrastructure and assistance offered by extremist organizations which can result into massive losses of human beings'lives and overwhelming material losses[5]. The open profile of the modern democratic societies, as well as the complex and contradictory way of the globalization tendency aspects, maintain the vulnerability to the international terrorism of both each separate state and of the whole international community[6].

The international terrorism places an ever increasingly pressure upon the democratic societies, forcing them to take steps to prevent and counteract it in more complex and tougher ways, facing even the risk to limit the fundamental human rights in their free exercise, to pervert in a way the democracy in such a way as to shake the trust of the peoples in its capacity to offer well being and security under freedom circumstances.

The terrorist violence must be understood not as a goal in itself, but as a way to reach a goal, a way to intimidate, to punish, to humiliate or to destroy[7]. In other words, "*the terrorist violence can be perceived as a form of political play where the act of violence and massacre produced represent a minutely directed script in order to communicate a certain message*"[8].

1. The Event

The 7th day of the Gregorian calendar normally represents a holly day for the Christians, as the Church celebrates John the Baptizer, as one of the major saints after Virgin Mary[9], considering him more than a prophet[10], namely "*the prophet of the Holiest*"[11], he was the one to announce the arrival of Christ, to baptize Him when he is there in order to accomplish GOD's plan.[12.]

---

[4]*Strategia de Securitate Naţională a României (National Security Strategy of Romania)*, Bucharest, 2006, page 8, available online at: http://presidency.ro/static/ordine/CSAT/SSNR.pdf, accessed on February 14, 2015.

[5]" *The National Security Strategy of the United States of America", President of the United States, White House, Washington DC, September 2002*, p.4, available online at: http://www.state.gov/documents/organization/63562.pdf, accessed on February 15, 2015.

[6]*Strategia de Securitate Naţională a României (National Security Strategy of Romania)*, Bucharest, 2006, pages 8-9, available online at: http://presidency.ro/static/ordine/CSAT/SSNR.pdf, accessed on February 14, 2015.

L. Ludmila Anica (Cîrnici), *Europe between state terrorism and individual terrorism – The shooting down of passenger aircraft MH17*. Article *on International Scientific Conference Strategies XXI*, The Complex and dynamic nature of the security environment, "Carol I" National Defence University, Centre for Defence and Security Strategic Studies, 25-26 November, 2014, Bucharest, p. 138, volumul I.

[8]W, Reich, *"Understanding terrorist Behavior: The Limits and 1 Opportunities of Psychological Inquiry"* edition *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*, 1998, Woodrow Wilson Center Press, Washington, DC, pp. 261-280.

[9]Ene Branişte; Ecaterina Branişte, *Dicţionar enciclopedic de cunoştinţe religioase (Encyclopedic Dictionary of the religious knowledge)*, "Diecezana" Publishing House, Oradea, 2001, p. 218, available online at: https://archive.org/stream/EneSiEcaterinaBraniste-DictionarEnciclopedicDeCunostinteReligioase#page/n215/mode/2up, accessed on February 15, 2015.

[10]*Ibidem.*

[11]*Ibidem.*

[12]Wikipedia, the free encyclopedia, available online at: http://ro.wikipedia.org/wiki/Ioan_Botez%C4%83torul,

The year 2015 brings a new understanding to this specific day after the Attack of the Charlie Hebdo, Paris, remaining in the collective memory as a mourning day for the French and not only for them. *Charlie Hebdo*, a French satirical weekly magazine, known for its profoundly provocative tone, unleashed frequently polemics, and among them, recently, those connected to the Islam. The most controversial caricatures published in this weekly magazine have been those connected to the prophet Mohamed[13].

The 7th of January, 2015 brought by the death in the families of the 12 sacrificed on "*The Altar of the Freedom of Speach",* among the victims we count five caricaturists, three editors, one press corrector, a worker and two policemen, one of the latter being the body-guard of the main caricaturist of the magazine (Charb) ever since 2011, after the publication of the caricatures with Mahomed[14], and the second, Ahmed Merabet, a Muslim, and a police officer of 42, was deadly shot outside, while he was firing back[15].

The attackers, dressed in black and wearing masks on their faces, entered in the head office armed with assault Kalashnikov weapons and practically, executed their victims: the editor in chief (the caricaturist Charb) being the main target of the bloody attack[16]. During the attack, another caricaturist, two journalists and several police officers have also been injured.

The witnesses say that the terrorists would have shouted "*Allah akbar",* an Arabic Islamic phrase called "*Takbir"*, meaning that "*God is almighty"* or that "*God is Big" or* "*God is the Biggest"[17],* after which they uttered in French that they have revenged Prophet Mahomed (*On a vengé le prophète Mohamed*!)[18].

After the attack, as per the statements of the French officials, the attackers left the magazine's headquarters, running towards a black C3 Citroen, and, to escape the police followers, they have abandoned the car somewhere in the north-east of Paris, near the park Buttes-Chaumont, disappearing on board of a stolen Renault Clio[19].

The main suspects, Cherif and Said Kourachi, two brothers with French citizenship but of Algerian origin, have been deadly shot during the shots between them and the special forces, after less than 54 hours since the terrorist attack. A third suspect, the brother-in-law of the first two, has been released after long hearings (almost ten hours), having been proved that he had no

---

accessed on 15 February 2015.

[13]Fran Blandy, "12 dead in 'terrorist' attack at Paris paper" article online website Yahoo News, published on January 7, 2015, available online at: http://news.yahoo.com/ten-dead-paris-newspaper-shooting-prosecutors-112635032.html, accessed 15 February 2015,

[14]The Guardian, Charlie Hebdo Attack Report, Tony Abbott condemns barbaric Charlie Hebdo attck in Paris, published on January 7, 2015, available online at: http://www.theguardian.com/world/2015/jan/08/tony-abbott-condemns-barbaric-charlie-hebdo-attack-paris, accessed on 15 February 2015.

[15]Newsweek online, Police Officer Shot During Charlie Hebdo Ahmed Merabet Massacre, published on January 7, 2015, available online at: http: //www.newsweek.com/officer-shot-during-charlie-hebdo-massacre-identified -297,603, accessed January 10, 2015.

[16]Rob Crilly, Raziye Akkoc, Unity Rally for Paris shootings: live Telegraph.co.uk. 8:45 PM GMT, January 11, 2015, available online at: http://www.telegraph.co.uk/news/worldnews/europe/france/11329976/Paris-Charlie-Hebdo-attack-live.html, accessed on 15 February 2015.

[17]Wikipedia, the free encyclopedia, Allahu Akbar (disambiguation), available online at: http://en.wikipedia.org/wiki/Allahu_Akbar_%28disambiguation%29, accessed on February 6, 2015.

[18]BBCNews Europe, on-line, published on January 7, 2015, available online at: http://www.bbc.com/news/world-europe-30710883, accessed on February 10, 2015.

[19] Patricia Tourancheau, *Un commando organisé, Liberation, Accueil, Société, Fusillade meurtrière à «Charlie Hebdo»* published on January 7, 2015, available online at: http://www.liberation.fr/societe/2015/01/07/un- commando-organic-et-prepare_1175841, accessed on 10 February 2015.

connection with the attack, as he attended courses at that moment[20].

2. National and international reactions

It goes without saying that, after such an attack and after such a shock, doubts appeared regarding the official version of the story of the event and also questions regarding some details which do not apparently link; for instance, it looked strange that two attackers, who prepared this attack minutely and who - as per the video records in-situ, had a very good military training, a precise and calm behavior – could possibly leave behind an ID, on the rear seat of the car. Therefore, if this ID belongs or not to the actual terrorist will ever be a doubt, circulated in the media.[21]

The international reactions appeared immediately, blaming this attack against the civilians, journalists, who – even if forcing the parody to its extremes – have judged that via their caricatures, they protect the freedom of religious choice; Gérard Biard, the present editor in chief, declared that such caricatures do nothing but ensure such freedom, as they *"declare that God must not be a political or public figure, but a private one[22]".*

Nevertheless, Pope Francis said that *"there are limits in the freedom of expression"[23]*. He said that the freedom of religious choice is a fundamental right of the human being and that *"nobody can provoke, or insult the religion of other people, nobody is free to mock another religion or religious faith"[24]*.

President Obama convicted the attack of the head-office of the French satirical magazine as an act of violence not only against the persons, but also against the idea of freedom of expression in the civilized world. He stated that *"for us, seeing such diabolic, coward attacks (...) underlines once again why it is so important for us to be in solidarity with them as they are in solidarity with us"[25],* namely, he underlines hereby the importance of cooperation with the allies in the fight against terrorism.

During the discussions with Vice-President Joe Biden and with State Secretary John Kerry, in one of the meetings in the Oval Office, Obama also added that *"the fact that this was an attack against the journalists, an attack upon our free journalism, highlights that these terrorists are afraid by the freedom of expression and the freedom of the press"[26]*.

---

[20]Wikipedia, The Free Encyclopedia, *Atentatul împotriva revistei Charlie Hebdo (Charlie Hebdo magazine attack)* available online at: http://ro.wikipedia.org/wiki/Atentatul_%C3%AEmpotriva_revistei_Charlie_Hebdo# Suspec.C8.9Bi, accessed on February 6, 2015.

[21]Article *Terrorist attack in Paris*. "L'Express" present (false) conspiracy theories, published online on 08.01.15, available online at: http://www.digi24.ro/Stiri/Digi24/Extern/Europa/ATAC+TERORIST+PARIS+teoriile+ plot, accessed on February 2, 2015.

[22]Elisha Fieldstadt, *Charlie Hebdo Cartoons Protect Freedom of Religion*, Editor Says NBC News Online, published online on January 18, 2015, available at: http://www.nbcnews.com/storyline/paris-magazine-attack, accessed on February 10, 2015

[23]Alexandru Matei: *Papa Francisc: Oricine ridiculizează credinţa cuiva se poate aştepta la un pumn (Pope Francis: Anyone ridicule one's faith can expect a punch)* published in Presa Liberă.net » Home»Social» on January 16, 2015, http://www.presalibera.net/papa-francisc-oricine-ridiculizeaza-credinta-cuiva-se-poate-astepta-la-un-pumn_1817703. html, accessed on 14 February 2015.

[24]Elisha Fieldstadt, art, cit.

[25]Weinberg, Ali: *Charlie Hebdo: President Obama Condemns' cowardly, 'Evil' Paris Attacks,* published in ABC News, *Good Morning America* via on January 7, 2015, available at: http://abcnews.go.com/News / obama-condemns-cowardly-evil-paris-attacks / story? id = 28058882, accessed on February 12, 2015.

[26]RFI Romania, *News, information, news live, international press*, available online: http://www.rfi.ro/node/54804/ and http://www.rfi.ro/presa-interna%C5 A3ional% C4% 83%? page = 69, accessed on February 14, 2015.

The American State Secretary John Kerry, toughly blamed the attack which targeted the head-office of Charlie Hebdo, reassuring, during a statement made in French, that *"the freedom of expression cannot be murdered"*[27].

François Hollandere proved *"a terrorist attack"* of an *"exceptional barbarism"*[28] and added that *"many (other) terrorist attacks have been annihilated during the past several weeks"*[29].

Other political leaders of the contemporary world condemned this terrorist attack, and some of them are Angela Merkel, David Cameron, Queen Elisabeth the 2nd, but also Jean Claude Junker, who rightly qualified it, as *" intolerable and a barbary"*[30].

The Russian President Vladimir Putin sent his condolences to President Francois Holande, for the loss of human lives caused by the terrorist attacks, blaming the barbarian act and expressing, as early as January, the 8th, *"the hope that the culprits will be punishedi"*[31].

"A terrorist act, bloody and coward" said the President of Romania, Klaus Iohannis, who expressed "*his compassion for the families of the victims*"[32]. He has also changed his profile photo on a socializing site with the already famous photo *"Je suis Charlie"*[33], representing *"the slogan of solidarity with the victims of the attack in Paris used on the socializing networks and on the site charliehebdo.fr after the attack"*[34].

If we are to remind here the definition given by Hoffman saying that *"all the acts of terrorism imply violence or the menace with violence and that terrorism is specially conceived to have psychological effects on a large scale, beyond the immediate victim/victims or the object of the terrorist attack, that it is meant to induce fear, and, as a sequence, to intimidate a much wider "target-public" which can include an ethnical or religious rival group, a whole country, a national government, political party or the public opinion, in general"*[35], we could say that the events taking place in Paris determined a reverse reaction within the population and that, beside the murder of the 12 in the magazine head-office, the attack has not totally reached its goals, unleashing a huge wave of disapproval and neutralizing desire.

Hoffman brings in the discussion the fact that terrorism is based on power and that it uses publicity to induce change, making use, on purpose, of fear via menace or violence, as well as of

---

[27]Article *Reacţiile oficialilor internaţionali după atacul terorist de la Paris*, *(Reactions international officials after the terrorist attack in Paris)* published online January 7, 2015 www.mediafax website, available online:http://www.mediafax.ro/externe/reactiile-oficialilor-internationali-dupa-atacul-terorist-de-la-paris-ban-ki-moon-e-un-atac-contra-democratiei-john-kerry-libertatea-de-exprimare-nu-poate-fi-ucisa-13752795, accessed on February 10, 2015.

[28]Wikipedia, The Free Encyclopedia, *Atentatul împotriva revistei Charlie Hebdo,* (*Charlie Hebdo magazine attack),* available online at: http://ro.wikipedia.org/wiki/Atentatul_%C3%AEmpotriva_revistei_Charlie_Hebdo, accessed on February 6, 2015.

[29]FRANCE 24 International News 24/7 online, *Manhunt after deadly terrorist attack Charlie Hebdo*, January 8, 2015, available at: http://www.france24.com/en/20150107-live-blog-gun-shots-french-paris-charlie-hebdo-satirical-magazine/ accessed February 14, 2015.

[30]RFI Romania, News, information, news live, international press, available online at: http://www.rfi.ro/presa-interna%C5%A3ional%C4%83?page=69, accessed on February 14, 2015.

[31]Official Internet Resources of the President of Russia, *Telephone conversation with President of France Francois Holande*, published on 08.01.2015, available online at: http://eng.kremlin.ru/news/23479, accessed on 01.10.2015.

[32]Wikipedia, The Free Encyclopedia, *Atentatul împotriva revistei Charlie Hebdo (Charlie Hebdo magazine attack)*, available online at: http://ro.wikipedia.org/wiki/Atentatul_%C3%AEmpotriva_revistei_Charlie_Hebdo, accessed on February 6, 2015.

[33]http://www.hotnews.ro/stiri-esential-19038290-klaus-iohannis-schimbat-poza-profil-sloganul-solidaritate-suis-charlie.htm.

[34] Wikipedia, the free encyclopedia, art, cit.

[35]Bruce Hoffman, *Inside Terrorism*, 2nd Edition, Columbia University Press, New York, 2006, p.27.

the psychological effects, beyond the target-groups. The fear is disseminated by mass-media and by our collective and individual feed-backs to the terrorist acts. The major part of the power of terrorism derives from the answer to the terrorist act and not from the act itself[36].

The population demonstrated to the terrorists that it will not let itself intimidated , attending, in Paris and in other communities, impressive silent marches (only in Paris we are talking of over 10,000 people), marches against terrorism, with participants wanting to show that they refuse to be afraid. They were carrying placard reading „Je suis Charlie" (I am Charlie). On the socializing networks they posted thousands of messages with the hash-tag #jesuischarlie[37].

The way we are answering back to terrorism after an event or incident is as important as to try to prevent it.

3. Analysis

Althought here are not divergent opinions on the diagnosis of the event ocurred on January the 7th 2015, wecould, at first, askourselves if we are talking here about a terrorist attack or only about a cruel and criminal manifestation of some individuals who has lost, for a while, the contact with reality or with human consciousness.

Today's specialized literature defines terrorism rather as a violent act, premeditated, achieved by conspiracy organizations with a distructive character, or by single persons against officials, political, economical, scientific, military, cultural,or diplomatic institutions in order to take revenge, in order to oblige the "target" to adopt an atitude convenient to the authors, to make sensible the public opinion in connection with a certain cause, to undermine the political stability and to satisfy some claims.

Starting from the conviction that the main characteristics of terror are violence and menace with violence, the systematic and persistant use of violence, intimidation and vulnerability via agressivness and hate, Christian Delanghe, stated in 2001 in "*La guerre contre la terrorism"* that*"terrorism is a problem of the people plunging in a logics of hatred without limits, for whom all the values founding our society and specially the respect toward the human life have no longer value"*[38]. Taking into account this definition, we can state, without any doubt, that it was indeed a terrorist attack.

Similar to the terrorist attacks against the Twin Towers on September the 11th 2011, which represented a historical major moment determining the re-thinking of democratic proceses and of those regarding the protection of the human rights, the re-evaluation of the connections with the globalization phenomena and of the approach of the core of the inter-civilizational relationships, and the attack upon the hesd-office of the French magazine highlights the paradox of the co-existance of the positive aspects of globalization (from the perspective of the evolution

[36]Wikipedia, the free encyclopedia, art, cit.

[37]Article *Atac Terorist Paris. Zeci de mii de persoane au ieşit în stradă (Terrorist attack in Paris Tens of thousands of people took to the streets)*, published online on January 1, 2015, available online at: http://www.digi24.ro/Stiri/Digi24/Extern/Europa/ATAC+TERORIST+PARIS+Zeci+de+mii+de+persoane+au+iesit+in+strada+d, accessed on February 2, 2015.

[38]Christian Delanghe, *La guerre contre le terrorisme,* 18.09.2001, available online: www.fr.strategie.org, accessed on January 18, 2015, was quoted by Gheorghe Văduva in volume *Terorismul. Dimensiune geopolitică şi geostrategică. Războiul terorist. Războiul împotriva terorismului (Terrorism. Geopolitical and geostrategic size. Terrorist war. The war against terrorism),* Security Center for Strategic Studies, Bucharest, 2002, p. 19, available online at: http://cssas.unap.ro/ro/pdf_studii/terorismul.pdf, accessed on January 18, 2015.

of modern technology) with the negative aspects embodied in the use, in a distructive way of such technologies.

As early as 2001 a new vision regarding the projected image of the "*new terrorism*" was generated, consisting in the definition of the moment 9/11 as being an actual re-wakening of the global society from a beautiful dream of globalization and its plunge in the nightmare of an anarchic globalization. For many anarchists, the terrorist attacks seem to confirm the alarm signal blown by Samuel Huntington, as per which the world would be on the threshold of unleashing "*a global war among civilizations, without battlefields and without frontiers*"[39].

It is of common knowledge that he anticipated that the wars of the future will not be among nations, but among civilizations, specially between the Occident (considered to be mostly Christian catholic and protestant, democratic, globalist, humanist, materialistic, secular, multi-cultural) and the Orient (seen as an mixture of Islam-orthodox, non-democratic, religiously conservative, religious, ideologized, intolerant, anti-globalist, anti-modernistic).[40]

Al-Qaida attacks, or those supposed to promote or to be sustained by al-Qaida have been shown, therefore, as being an inevitable fundamentalist reaction to ward the contemporary modernity and technological progress, and, as a sequence, the main source of suffering and frustration of the traditional civilizations (Oriental, Islamic, Assian) menaced to be swallowed by the American and Western-European civilization seen as materialistically vulgar, comsumeristic and immoral.

The ideologists of the new terrorism display the Oriental world (using as argument the sketch of global bang drawn by Huntington) as being (because of the western agression and domination for over one thousand years) in a dramatic decline, in an peripheric position, technologically obsolete and incapable in front of the expansionistic provocations of what they call the Euro-Atlantic imperialism.[41] Thesevisions, fed by the unfightable reality of the tragic event, focussed the attention on this type of terrorism (Islamic fundamentalist), launching it as the main (and overwhelming) menace to ward the security of the community.

Hence, the main positive effect was a rapid and efficient coagulation of the efforts of the majority of national and international actors on the barricade of rejecting this type of catastrophic violence.[42]

A bigger and bigger pressure is felt by the democratic societies, obliging them to take steps towards more complex and tougher prevention and counter acting measures, facing the risk to limit the free exercise of the fundamental human rights, to issue a pervert democracy meant to decrease the trust of poeples in its capacity to offer well fare and security under freedom circumstances. Subsequently, in such a complex situation, fluid and subject to uncertainties, the „must" of counteracting this flagel and of the cooperation of democratic forces to face it – here included mutual actions deployed in the areas generating the main acts of terrorism - becomes vital[43]. Under the circumstances of the present security environment, terrorism, through its effects and consequencies, endangers the very existance of the universal human values. The

[39]Glen E Perry, "Huntington and his critics: the Occident and Islam", in Samuel P. Huntington, *Arab Studies Quartely*, Winter 2002.
[40]Langman, Lauren, Moris, Douglas., *Islamic Terrorism: From Retrenchment to Ressentiment and Beyond*, Loyola University Press, Chicago, 2002.
[41]Graham E. Fuller, *The Future of Political Islam*, Palgrave Macmillan Ed, New York 2004.
[42]Jeffrey Record, *Bounding the Global War on Terrorism,* Strategic Studies Institute, New York, December 2003.
[43]*Strategia de Securitate Națională a României* (*National Security Strategy of Romania)*, Bucharest, 2006, pages 8-9, available online: http://presidency.ro/static/ordine/CSAT/SSNR.pdf, accessed on 14 February 2015.

unprecedented explosion of the terrorist acts imposed the reaction of the international community, which, more solid and more united than ever[44], unleashed the fight against terrorism.

The new menace, as well as the reaction of the international community toward it, have major implications and consequences upon all domains of social life, but specially upon the way in which the political responsibles decide the engagement and the use of military capacities in the future operations of fighting back the terrorism.

Hoffman suggests touchable elements in defining the phenomenon:"*All terrorist acts imply violence or menace with violence. (...) Terrorism is meant to generate power where it doesn't exist, or to consolidate it where it is very poor. By the publicity generated by violence, the terrorists seek to get influence, power and control which they don't possess, to impose a political change, on a local or international scale"*[45].

In the same spirit, Paul R. Pillar lists, in his book "*Terrorism and U.S. Foreign Policy*" –a work published in 2001 in Washington, the following four main elements which can be found in the majority of definitions used by the authorities implied in counteracting the terrorism. As per the author's opinions, "*we can summarize four elements of terrorism which appear in the governmental definitions*[46]", without pretending that these are the absolute and only truth. They are:

- *"Premeditation – there must be an intention and a previous decision before an attack which could be called terrorist attack- terrorism is not provoked by spontaneous fury or by a spot impulse.*

- *Political motivation – criminal violence motivated by financial gains or personal revenge is excluded.*

- *Victims are non-combat persons – the terrorists attack persons which cannot fight back with the same violent means.*

- *The authors are either sub-national groups or private agents"*[47].

Conclusions

The brothers Cherif and Said Kourachi premeditated their action, minutely, aiming some non-combat persons (the head-office of the Paris magazine), making public their punishing message toward the caricaturists who dared to insult prophet Mahomed, shouting that "*God is almighty", or "God id (the most) almighty"*[48] and that they revenged the Prophet[49], therefore, their attack can be labeled, without doubt, as a terrorist attack.

Nowadays, of course, terrorism – under its multiple forms- is considered, in many occasions as being an asymmetrical attack of the weak against the strong, while, as an act of spectacular violence, terrorism is meant to convey a message: the authors feel that they do not have any other way to make themselves heard and they decide to convey their message, although,

---

[44]Anghel Andreescu; Nicolae Radu, *Organizaţiile teroriste, Conceptualizarea terorii versus securitatea europeană, (Terrorist organizations, conceptualization terror versus European security*), MIRA Publishing House Bucharest, 2008, available online at:
http://www.editura.mai.gov.ro/documente/biblioteca/2008/organizatii%20teroriste/organizatii%20teroriste.pdf, accessed on 20 February 2015.

[45]Bruce Hoffman, *Inside Terrorism*, 2nd Edition, , Columbia University Press, New York, 2006, p.27.

[46]Paul R. Pillar, *Terrorism and U.S. Foreign Policy,* Brookings Institution Press, Washington, 2001. pp. 13-14.

[47]Paul R. Pillar, *op. cit.*

[48]Wikipedia, the free encyclopedia, Allahu Akbar (disambiguation), available online: http://en.wikipedia.org/wiki/Allahu_Akbar_%28disambiguation%29, accessed on February 6, 2015.

[49]*Ibidem.*

in most cases, the public perception will be totally different to what they really want[50].

This premeditated act with the declared goal of revenge, had as object to oblige the" target" to adopt a position convenient to the authors, to impress the public opinion in connection with a certain cause, to undermine the political stability and to satisfy some claims. George Friedman explains in his article "*Paris Attack Underscores a Deeper Malaise*", published in Stratford Geopolitical Diary on January the 8th 2015, that, irrespective of the nature of such attacks – in the sense that they are connected or not with the Jihadists, - they have as result the depreciation of the existing tensions in the relationships between the Occidental and the Islam worlds, this being even more important in Europe, where *"the states are confronted with an increase of the right-wing nationalism and the Muslim communities are very dissatisfied"*[51].

Even more, we can feel a long-term conflict between the values of the two cultures and civilizations (Christian vs. Muslim) regarding the freedom of expression, which is extremely valued by the western world, but perceived by *"a lot of Muslim as a licence (abuse of liberty) for sacriledge"*[52]. The fact that the majority of Muslims will not engage in accomplishing some violence as a reply to the discourse considered a blasphemy; -still, some have done it and will probably do it again - to the origin of this attitude, we can find the extreme discomfort felt by the Muslims in connection with the "freedom of expression" regarding the Prophet, in the traditional vision this being impossible to describe in a picture-like way, more the less in a satirical way.

For the European Union the prevention and counteracting of terrorism demands a survey of the movements of the individuals and of the financial flows, although the European construction suppose, on the contrary, the fundamental principle of free circulation of persons and goods[53].

Moreover, the European project was built on the idea of giving up the war concept, having peace as horizon in all initially taken actions[54]. In the context where the security issues aim the legitimacy matter first, the fight against terrorism should follow different stages; thus, the European cooperation regarding the anti-terrorist fight- considered for a long time informal at the Union level- was always strongly activated within the frame of the European Council. But its competencies developed as a reply to autonomous or revolutionary terrorism and less in order to counteract the increase of the present day Islamic and international terrorism[55].

In connection with terrorism, the main means of action of the Union are the legislative alignment, the operational coordination of the services of the member states and the dialogue with third countries[56]. Among the first measures we can count: the strengthening of the financial and police cooperationby *initiating an European arrest mandate*, the identification of the terrorists by means of a *common list of the terrorist organizations,* creating a *team of anti-terrorists specialists* which should cooperate tightly with their American partners, applying

[50]Constantin Mostoflei, "Riscuri şi ameninţări actuale: între criză economică şi terorism" (*"*Risks and threats: between economic crisis and terrorism"), in *Securitate şi stabilitate regională (.Security and regional stability)* "Carol I" National Defence University Publishing House, Bucharest, 2009.

[51]Article *Paris Attack Underscores a Deeper Malaise,* published on January 8, 2015, in Geopolitical Diary, on STRATFOR Global Intelligence, available online at: https://www.stratfor.com/geopolitical-diary/paris-attack-underscores-deeper-malaise#axzz3O9XqOvot, accessed on March 10, 2015.

[52]Constantin Mostoflei, art. cit.

[53]Wilkinson, Paul, *International terrorism: the changing threat and the EU's response*, publicat European Union Institute for Security Studies, Bruxelles, October 2005, p.5, available online at: http://www.iss.europa.eu/uploads/media/ cp084.pdf, accessed on March 10, 2015.

[54]Constantin Mostoflei, art. cit.

[55]Alexandre Adam, *La lutte contre le terrorisme: étude comparative Union Européenne*, Ed. Harmattan, 2005, p. 30.

[56]*Ibidem*, pp. 14-17.

promptly *all international conventionsin anti-terrorist fight field,* fighting against *financing terrorism and strengthening of the air-services security*[57]. The anti-terrorist fight can be seen, as Alexandre Adam states in his work, as a *"catalystof the efforts to create a juridical European space which circumscribed, from the beginning, in the criminal logics*[58].

Nevertheless, the case Charlie Hebdo demonstrates, once again, that terrorism can appear anywhere and anytime, unexpectedly and surprisingly. Good and Evil are within us and it is hard to predict with certainty, which is the dominant feature in everybody's consciousness, because "*terrorism is a problem of human beings which plunge in a logics of unlimited hatred, for which all values functioning in our occidental society, and specially the respect toward human life has no longer a value"*[59].

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".", coordinated by the National Defence University "Carol I".

BIBLIOGRAPHY:

1. ADAM, Alexandre, *La lutte contre le terrorisme: étude comparative Union Européenne*, Ed. Harmattan, 2005, p. 30.
2. ALEXANDRU, Matei. *Papa Francisc: Oricine ridiculizează credinţa cuiva se poate aştepta la un pumn (Pope Francis: Anyone ridicule one's faith can expect a punch)*, published in Presa Liberă.net » Home » Social » on January 16, 2015, available online at: http://www.presalibera.net/papa-francisc-oricine-ridiculizeaza-credinta-cuiva-se-poate-astepta-la-un-pumn_1817703.html.
3. ANDREESCU, Anghel; RADU, Nicolae. *Organizaţiile teroriste, Conceptualizarea terorii versus securitatea europeană (Terrorist organizations, conceptualization terror versus European security)* M.I.R.A. Publishing House Bucureşti, 2008,

[57]*Joint Declaration by the Heads of State and Government of the European Union, the President of the European Parliament, the President of the European Commission, and the High Representative for the Common Foreign and Security Policy* , published on 14 September 2001, available online at: http://www.europa-eu-un.org/articles/fr/article_46_fr.htm, accessed on March 10, 2015.
[58]Alexandre Adam, *La lutte contre le terrorisme: étude comparative Union Européenne*, Ed. Harmattan, 2005, p. 30.
[59]Christian Delanghe, *La guerre contre le terrorisme,* 18.09.2001, available online: www.fr.strategie.org, accessed on January 18, 2015.

available online at: http://www.editura.mai.gov.ro/documente/biblioteca/2008/organizatii%20teroriste/organizatii%20teroriste.pdf.
4. ANICA (Cîrnici), L. Ludmila. *Europe between state terrorism and individual terrorism – The shooting down of passenger aircraft MH17*. Article *on International Scientific Conference Strategies XXI*, The Complex and dynamic nature of the security environment, "Carol I" National Defence University, Centre for Defence and Security Strategic Studies, 25-26 November, 2014, Bucharest, p. 138, volume I.
5. ATANASIU, Mirela; REPEZ, Filofteia. *Securitatea şi apărarea ţării în contextul ameninţărilor teroriste (Security and defense of the country in the context of terrorist threats),* "Carol I" National Defence University Publishing House, 2013, Bucharest, available online at: http://cssas.unap.ro/ro/pdf_studii/securitatea_si_apararea_tarii_in_contextul_amenintarilor_teroriste.pdf.
6. BLANDY, Fran.*"12 dead in 'terrorist' attack at Paris paper"*, Article on Yahoo News site, published on January 7, 2015, available online at: http://news.yahoo.com/ten-dead-paris-newspaper-shooting-prosecutors-112635032.html.
7. BRANIŞTE, Ene; BRANIŞTE, Ecaterina. *Dicţionar enciclopedic de cunoştinţe religioase (Encyclopaedic Dictionary of Religious Knowledge)*, Diecezana Publishing House, Oradea, 2001, p. 218, accessed on February 15, 2015, available online at: https://archive.org/stream/EneSiEcaterinaBraniste+DictionarEnciclopedicDeCunostinteReligioase#page/n215/mode/2up.
8. CRILLY, Rob; AKKOC, Raziye. *Unity rally for Paris shootings: live, Telegraph.co.uk*, published on January 11, 2015, available online at: http://www.telegraph.co.uk/news/worldnews/europe/france/11329976/Paris-Charlie-Hebdo-attack-live.html.
9. DELANGHE, Christian. *La guerre contre le terrorisme,* 18.09.2001, available online at: www.fr.strategie.org.
10. FIELDSTADT, Elisha. *Charlie Hebdo Cartoons Protect Freedom of Religion, Editor Says*, NBC News online, published on January 18, 2015, available online at: http://www.nbcnews.com/storyline/paris-magazine-attack.
11. FULLER, Graham E. *The Future of Political Islam*, Palgrave Macmillan Ed, New York 2004.
12. HOFFMAN, Bruce. *Inside Terrorism*, 2nd Edition, Columbia University Press, New York, 2006, p.27.
13. LANGMAN, Lauren; MORIS, Douglas. *Islamic Terrorism: From Retrenchment to Ressentiment and Beyond*, Loyola University Press, Chicago, 2002.
14. MOSOFLEI, Constantin, "Riscuri şi ameninţări actuale: între criză economică şi terorism" (Risks and threats: between economic crisis and terrorism), in *Securitate şi stabilitate regională (Security and Regional Stability).* "Carol I" National Defence University Publishing House, Bucharest, 2009.
15. PERRY, Glen E. "Huntington and his critics: the Occident and Islam"*,* in Samuel P. Huntington, *Arab Studies Quartely*, Winter 2002.
16. PILLAR, Paul R., *Terrorism and U.S. Foreign Policy,* Brookings Institution Press, Washington, 2001. pp. 13-14.
17. RECORD, Jeffrey. *Bounding the Global War on Terrorism,* Strategic Studies Institute, New York, Decembrie 2003.

18. REICH, W. *"Understanding terrorist Behavior: The Limits and 1 Opportunities of Psychological Inquiry"* in Edition *Origins of Terrorism: Psychologies, Ideologies, Theologies, State of Mind*, 1998, Woodrow Wilson Center Press, Washington, DC, pp. 261-280.
19. TOURANCHEAU, Patricia. *Un commando organisé,* Liberation, Accueil, Société, Fusillade meurtrière à «Charlie Hebdo» January 7, 2015, available online at: http://www.liberation.fr/societe/2015/01/07/un-commando-organise-et-prepare_1175841.
20. VĂDUVA, Gheorghe, *Terorismul. Dimensiune geopolitică şi geostrategică. Războiul terorist. Războiul împotriva terorismului (Terrorism. Geopolitical and geostrategic size. Terrorist war. The war against terrorism),* Security Center for Strategic Studies, Bucharest, 2002, p.19, available online at: http://cssas.unap.ro/ro/pdf_studii/terorismul.pdf.
21. WEINBERG, Ali: "*Charlie Hebdo: President Obama Condemns 'Cowardly,' 'Evil' Paris Attacks*" published in ABC News, via Good Morning America, on January 7, 2015, available online at: http://abcnews.go.com/News/obama-condemns-cowardly-evil-paris-attacks/story?id=28058882.
22. WILKINSON, Paul, *International terrorism: the changing threat and the EU's response*, published by European Union Institute for Security Studies, Bruxelles, October 2005, p.5, available online at: http://www.iss.europa.eu/uploads/media/cp084.pdf.

I N D E X

”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, Bucharest
e-mail editura@unap.ro
Tel: 021/319.40.80/453

642/2015 C. 245/2015