"CAROL I" NATIONAL DEFENCE UNIVERSITY
CENTRE FOR DEFENCE AND SECURITY STRATEGIC STUDIES

STRATEGIC IMPACT

No. 2[63]/2017

Academic quarterly acknowledged by CNATDCU,
Indexed in CEEOL, ProQuest, EBSCO, IndexCopernicus,
WorldCat and ROAD ISSN international databases

"CAROL I" NATIONAL DEFENCE UNIVERSITY PUBLISHING HOUSE
BUCHAREST, ROMANIA

EDITORIAL COUNCIL

Gheorghe CALOPĂREANU, PhD Professor, “Carol I” National Defence University, Romania, Chairman
Daniel DUMITRU, PhD Professor, “Carol I” National Defence University, Romania
Iulian MARTIN, PhD Professor, “Carol I” National Defence University, Romania
Valentin DRAGOMIRESCU, PhD Professor, “Carol I” National Defence University, Romania
Ion PURICEL, PhD Professor, “Carol I” National Defence University, Romania
Florian CÎRCIUMARU, PhD Lecturer, “Carol I” National Defence University, Romania
Florian RĂPAN, PhD Professor, “Dimitrie Cantemir” Christian University, Romania
Florin DIACONU, PhD Associate Professor, University of Bucharest, Romania
John F. TROXELL, Research Professor, Strategic Studies Institute, US Army War College
Adrian GHEORGHE, PhD Professor Eng., Old Dominion University, USA
John L. CLARKE, PhD Professor, “George C. Marshall” European Centre for Security Studies, Germany
Dariusz KOZERAWSKI, PhD Professor, National Defence University, Poland
Bohuslav PRIKRYL, PhD Professor, National Defence University, Czech Republic
Pavel NECAS, PhD Professor Eng., University of Security Management, Slovakia
Ilias ILIOPOULOS, PhD Professor, Naval War College, Greece
Gábor BOLDIZSÁR, PhD, National University of Public Service, Hungary
Péter TÁLAS, PhD, National University of Public Service, Hungary
Georgi DIMOV, PhD Associate Professor, “G. S. Rakovski” National Defence College, Bulgaria
Igor SOFRONESCU, Military Academy “Alexandru cel Bun”, Republic of Moldova

SCIENTIFIC BOARD

Stan ANTON, PhD, Lecturer
Mirela ATANASIU, PhD, Senior Researcher
Cristian BĂHNĂREANU, PhD, Senior Researcher
Cristina BOGZEANU, PhD, Senior Researcher
Ecaterina MAȚOI, PhD, Lecturer
Constantin MOŞTOFLEI, PhD Senior Researcher
Visarion NEAGOE, PhD, Professor
Marius-Titi POTÎRNICHE PhD, Researcher
Filofteia REPEZ, PhD, Professor
Alexandra SARCINSCHI, PhD, Senior Researcher
Cătălina TODOR, Junior Researcher
Dănuț TURCU, PhD, Professor
Eduard VITALIS, PhD, Lecturer
Mihai ZODIAN, PhD, Researcher

EDITORS

Editor in chief: Florian CÎRCIUMARU, PhD
Deputy editor in chief: Daniela RĂPAN, PhD
IDB dissemination: Andra-Ioana PÎNZARIU

Contact address:

Şoseaua Panduri, nr. 68-72, Sector 5, Bucureşti, România
Telephone: +4021-319.56.49, Fax: 4021-319.57.80
Websites: http://cssas.unap.ro/index_en.htm, http://cssas.unap.ro/en/periodicals.htm

Disclaimer:
Opinions expressed within published materials belong strictly to authors and do not represent the position of CDSSS/ “Carol I” NDU.
Authors are fully responsible for their articles’ content, according to the provisions of Law no. 206/2004 regarding good conduct in scientific research, technological development and innovation.

ISSN 1842-9904; ISSN-L 1841-5784

CONTENTS

EDITOR'S NOTE 5

POLITICAL-MILITARY TOPICALITY

Hybrid Conduct Determinations in the Current International System and the New Types of Threats Derived from Emergent Conflicts..7
Teodor FRUNZETI, PhD
Cristian BĂRBULESCU

GEOPOLITICS AND GEOSTRATEGY: TRENDS AND PERSPECTIVES

Bahrain's Role in the Geostrategic Vision of Iran and Saudi Arabia 17
Răzvan MUNTEANU

The Topicality of Security Dilemma's Spiral Model in Analysing the International Environment... 24
Cătălina TODOR

SECURITY AND MILITARY STRATEGY

Institutional Resilience Growth to Counter National Security Threats...............................34
Ștefan SĂVULESCU
Mihaela ȚONE

Advanced Model for Configuring Hybrid Aggression 45
Dan-Lucian PETRESCU

DEFENCE & SECURITY CONCEPTS

Conceptual Approaches to Cyberspace in NATO, EU and Romania..................................52
Mirela ATANASIU, PhD

Mathematical models specific to the military domain...62
Florentina-Loredana DRAGOMIR, PhD

SCIENTIFIC EVENT

International Symposium "Inter-institutional Cooperation – A Tool for Achieving Security at National and International Levels", 25 May 2017 68
Andra PÎNZARIU

CDSSS AGENDA

Activities of the Centre for Defence and Security Strategic Studies APRIL-JUNE 70
Raluca STAN

GUIDE FOR AUTHORS.. 72
Daniela RĂPAN, PhD

EDITOR'S NOTE

The second edition in 2017, no. 63, comprises a collection of seven papers, to these adding the traditional *CDSSS Agenda, Scientific event* and *the Guide for authors*.

The journal is opened by the rubric ***Political-military Topicality***, where General (r) Teodor Frunzeti and Mr. Cristian Bărbulescu reveal a series of *hybrid conduct determinations in the current international system and the new types of threats derived from emergent conflicts.*

At the rubric ***Geopolitics and Geostrategy: Trends and Perspectives***, our colleague, Cătălina Todor, Junior Researcher, shares with you the results of her study on *the topicality of security dilemma's spiral model in analysing the international environment.*

In the following, Mr. Răzvan Munteanu provides an analysis of *Bahrain's role in the geostrategic vision of Iran and Saudi Arabia*.

Next comes the rubric ***Security and Military Strategy***, where you can read the material elaborated in co-authorship by Police Chief Commissioner Ștefan Săvulescu and Mrs. Police Commissioner Mihaela Țone, on *institutional resilience growth to counter national security threats*, which was delivered at the Symposium organised by CDSSS on 25 May 2017.

In the second article, Lieutenant-colonel Dan-Lucian Petrescu dwells on an *advanced model for configuring hybrid aggression.*

At the rubric titled ***Defence and Security Concepts***, we included two articles, the first belonging to our colleague, Mirela Atanasiu, PhD Senior Researcher, approaching *conceptual approaches to cyberspace in NATO, EU and Romania.*

In the second article, Mrs. Florentina-Loredana Dragomir, PhD Lecturer presents a series of *mathematical models specific to the military domain.*

Our new colleague Andra Pînzariu, presents in the rubric ***Scientific Event***, a few conclusions after *International Symposium "Inter-institutional Cooperation – A Tool for Achieving Security at National and International Levels"*, organised by CDSSS on 25 May 2017.

CDSSS Agenda for the period April-June is brought to your attention by Ms. Raluca Stan.

In the end, Mrs. Daniela Răpan, PhD signals the ***Guide for Authors***, a useful lecture for those interested to disseminate the results of their research in *Strategic Impact* quarterly.

For those who open *Strategic Impact* for the first time, we mention that the journal is an open access publication of the Centre for Defence and Security Strategic Studies within "Carol I" National Defence University (available at http://cssas.unap.ro/en/periodicals.htm) and is a *prestigious scientific journal in the field of Military Science, Information and Public Order*, according to National Council for the Recognition of University Degrees, Diplomas and Certificates (CNATDCU).

The journal is being published four times per year, for 17 years in Romanian and for 13 years in English, approaching a complex thematic: security and defence related issues; security and military strategies; NATO and EU policies, strategies and actions; political-military topicality; geopolitics and international relations; future of conflict; peace and war; information society, intelligence community. Readers may find, in the published pages, analyses, syntheses and evaluations of strategic level, points of view which study the impact of national, regional and global actions dynamics.

The journal is distributed free of charge in main security and defence institutions, as well as in national and international academia in Europe, Asia and America.

Regarding international visibility – an important objective of the journal –, recognition of the publication's scientific quality is confirmed by its indexing in the international databases CEEOL (Central and Eastern European Online Library, Germany), EBSCO (USA), ProQuest (USA), Index Copernicus International (Poland), WorldCat and ROAD ISSN, but also by its presence in virtual catalogues of libraries of prestigious institutions abroad such as NATO and of universities with military profile from Bulgaria, Poland, Czech Republic, Hungary, Estonia and so on.

I hope that this brief introduction shall act as a stimulus not only to read this issue of the journal, but also to inspire you with new topics to tackle in your research endeavours, which we look forward to receiving for the prospect of future inclusion in *Strategic Impact* and in *Strategies XXI International Scientific Conference*.

Further on, we are sharing with our readers the fact that there have been some changes in the componence of the Editorial Council and the Editorial Team, as a consequence of the retirement of a few members of our academic leadership, including CDSSS former Director and Editor-in-Chief of Strategic Impact, Colonel Stan Anton, PhD.

The Editorial Council welcomes thus the new NDU Prorector for Scientific Research, Colonel Iulian Martin, PhD, the new President of The NDU Senate, Colonel Ion Puricel, PhD and last but not least, of Colonel (Ret.) John F. Troxell, Research Professor with Strategic Studies Institute/ US Army War College.

The current Acting Director of the Centre for Defence and Security Strategic Studies and Editor-in-Chief of Strategic Impact is Colonel Florian Cîrciumaru, PhD.

The main objective that the editors have set for the period to come is to consolidate and broaden relations with institutions and research centres both at national and worldwide level.

We hope that this introduction shall act as a motivation not only to read this issue of the journal, but also to inspire you with new topics for your research endeavours, which we look forward to receiving for the prospect publication in *Strategic Impact and in Strategies XXI International Scientific Conference.*

The Editors

HYBRID CONDUCT DETERMINATIONS IN THE CURRENT INTERNATIONAL SYSTEM AND THE NEW TYPES OF THREATS DERIVED FROM EMERGENT CONFLICTS

Teodor FRUNZETI, Ph.D *
Cristian BĂRBULESCU**

Recent developments in the global security environment - such as the crisis in Ukraine and the terrorism resurgence - have reopened the international relations (IR) and security studies debates on the reconfiguration of the international system and the emergence of the revolutionary changes in modern warfare.

This paper highlights how geostrategic competition shapes the actors' hybrid assertive conduct within the international system. We will describe how the confrontations between actors are influenced by the remodeling tendencies and manifestations in the international system and we will point out that the hybrid and diffuse actions, located at the boundary between peace and war, remain a valid option for the emerging actors to contesting the influence of the globally dominant power (aiming to legitimize the multipolar international system).

Keywords: *multipolar international system, emergent conflicts, state actor, non-state actor, hybrid threats.*

1. Preliminary considerations

The current international system goes through a structural transformation timeframe with implications on both its core and elements - actors, size, structure, processes and interaction capacity[1]. Transformation is irreversible and is generated by discontinuities taking place permanently on the *actors'* side (which determine their evolution or involution) and on the *relations* between them, which ultimately leads to the continuous regeneration of the international system.

Most of the recent reports on the international system transformation are reduced to the changing of the dominant power or polarity thesis, although the process *per se* implies a lot more than

[1] The conceptual framework proposed by Barry Buzan is particularly useful in understanding the developments that shape the international system. It highlights the levels (international system, subsystems, units, etc.) and the analysis sectors (political, military, economic, socio-cultural and environmental) and sources of explanation (process, interaction and structure) as working tools for the analysis of the developments within the global international system.

****Teodor FRUNZETI is PhD Professor with "Titu Maiorescu" University and a Member of the Academy of the Romanian Scientists in Bucharest, Romania. E-mail: tfrunzeti@gmail.com***

*****Cristian BĂRBULESCU is PhD Student at "Carol I" National Defence University and a Research Assistant with the Academy of the Romanian Scientists in Bucharest, Romania. E-mail: cebarbulescu@gmail.com***

that as variations are highly visible in multiple domains of interaction (e.g. technological, informational, political, economic and military). Our analysis starts from the premise that the changes taking place in the international system concern the *dominant processes* within – political, military, economic, socio-cultural.

2. Emerging trends in international relations

The representation of the three dominant IR theories – *structural realism* (or neorealism), *neoliberalism* and *constructivism* coexists and interferes within the current international system. Shading differences are what preserves the "competition" between them. *Realism*, which states that in an anarchic system the actor himself is the only one who can provide his own security and contribute to maintaining balance in the international system, differentiates from the *liberal* view, which supports the values and norms power within the IR, and *constructivism*, that promotes the idea that, under anarchy conditions, the identity and interests of the actors derive from their interactions, which are conducted by the rules of the environment.

Neorealism seems to be still a dominant in IR. The international system remains dominated by the state actors' capacity of influence and power projection. The chaos in the international system is maintained by the conduct of state actors seeking to satisfy their own interests in the interactions they create with other actors and also by the absence of a supranational "institution" to deter states' egocentric tendencies. On the other hand, *the exponential growth of political, economic and social interconnection, in conjunction with the acceleration of the globalization process and the advance of technological innovations, keeps up feasible the neoliberal options in IR* – based on economic and community values, regional integrated projects and the efforts to develop a framework that would have to set the rules for the interactions in domains still underexplored, such as climate change and cyberspace.

Immediately after the end of the Cold War, Barry Buzan pointed out that the new structure of power relations is multipolar, in that many independent powers are at stake, but unipolar due to the presence of a single dominant power center governing the international relations (which we consider to be the US-led western coalition)[2]. The collapse of the Soviet Union has caused the bipolar reality breakdown and the end of confrontation between the two major political-military blocs, NATO and the Warsaw Treaty. It marked the beginning of unipolarity in the international system. Unipolarity is, in our view, a transitional phase towards a polycentric power distribution system at a global level. The reality described by the assumption of global leadership by only one great power remains valid if two essential conditions are satisfied. First, this type of commitment should fulfill its direct interest through the political and economic leverage it might generate. On the other hand, there should be no other great power which is able to achieve this kind of role or proves not to be interested to accept it. However, it is difficult today to assess whether this intermediate step has been or not fully covered. From a military perspective, we believe that the international system is still unipolar, as it continues to be dominated by a single great power, namely the United States (US), which has a tremendous global power projection capability. We also consider that a broad picture of the international system could be attained only by overlaying together the political, economic and socio-cultural dimensions. The representation we get reflects the presence of several competing regional power centers (US, Europe, Russia, India, China) combined with some other sources of instability (in Eastern Europe, Caucasus, Middle East and North Africa, Asia-Pacific).

The challenge of the dominant power center (currently associated with the US and the West) will certainly influence the configuration of future arrangements within the international system. *The realistic scenario of a polycentric*

[2] Barry Buzan, *New Patterns of Global Security in the Twenty-First Century*, International Affairs (Royal Institute of International Affairs 1944-), Vol. 67, No. 3 (Jul.,1991), p. 437, available on http://www.jstor.org/stable/2621945, accessed on 06.05.2017.

world based on the balance of power between the various political-economic and regional military centers is supported by the recent developments. Nowadays it is becoming more and more difficult to implement the United Nations liberal policies and programs devoted to international and regional stability. The assertive policies of the emerging great powers (like China and Russia) and the propensity for emphasizing the regional and global profile of the political-economic organizations (EU, Economic Eurasian Union / EEU, Association of South-East Asian Nations/ASEAN) will become more and more obvious. This scenario will be accepted also by the supra-state entities (EU, ASEAN, UEE) which were born based on the principles of neoliberalism. They will not give up on the values that define their existence but will seek to achieve "personality" into the new system of IR, becoming ever more politically involved at regional and global level. Indeed, defining the personality within the international system is an end-state already assumed at EU level, the most advanced regional project of political and economic integration, being included in the EU Global Strategy (2016)[3].

In our opinion, the recognition of the post-modern polycentric power distribution system will not necessarily lead to the decline of the liberal ideas on IR. On the contrary, this scenario reflects the *survival of the integrative liberal model in a multipolar world. The new post-modern world order and IR will function as a hybrid through the symbiosis of both the liberal and neorealism principles.*

The new world order will lead to *turning the global geostrategic competition to the regional level of interactions.* This perspective is favored by the recurrence of the economic stakes in the relations between actors and regional and inter-regional market integration (e.g. Chinese Silk Road Initiative, Comprehensive Economic and Trade Agreement / CETA between EU and Canada, the Transpacific Agreement). We say, therefore, that the *international system follows a stage of structural transformation*, because for the most part of it, the major change comes from the concentration of policies regionally (on the political and economic sectors). In this scenario the military dimension is not minimized but serves the fulfillment of the political and economic interests of the competing actors. The complementarity of the two dimensions, economic and military, reflected by the combination of "soft" and "hard" power instruments, is also a trend in IR. The rapid technological changes increase the level of global interconnection, especially, in the social and economic domains. From a social perspective, the multiplying communication options within communities, states and beyond define the reality of the *information society* in which we live. On the other side, the relatively slow economic growth of the US (2.2%) and the EU (2.3%) compared with the Asian countries – China (6.8%), India (7.1%), Indonesia (5.2%) – which is to be maintained as a trend for the next decade[4], emphasizes the nationalist and protectionist reflexes in Western societies. However, economic power is not the only driver that contributes to the global balance of power, but it is certainly one of the most influential. The economic driver contributes to a great extent to the consolidation and development of the military capabilities of the competing great players (US, on the one hand, and China and Russia on the other hand – whose military expenditure has doubled over the last ten years[5]).

From this point of view, it remains relevant how the conflict will be reflected in the upcoming confrontational relations, what are the factors shaping the actors aggressions and whether there exists any connection between the actors' hybrid activities and the IR dynamics.

[3] provides for the promotion of European values and interests (peace and security, democracy and a global rule-based order) on a global scale. *European Union Global Strategy*, June 2016, p. 13, available on eeas.europa.eu/archives/docs/top.../eugs_review_web.pdf, accessed on 12.10.2017.

[4] *World Economic Outlook (October 2017)*, International Monetary Fund, available on http://www.imf.org/external/datamapper/ngdp_rpch@weo/oemdc/weoworld/chn/usa/advec/eu/as5/da/bra/ind, accessed on 30.11.2017.

[5] *SIPRI Military Expenditure Database*, Stockholm International Peace Research Institute, available on https://www.sipri.org/databases/milex, accessed on 30.11.2017.

3. Key-drivers capable to generate change in the international system

3.1. Technological innovations

The current information society is the product of the innovations generated by the "Fourth Technological Revolution"[6]. Merging physical computing systems with data processing and communication networks and, in addition, the high degree of interaction between intelligent technologies and the human factor can generate security challenges. Technology creates mutations in warfare[7]. In post-modern conflicts, the distinction between peace and war, between combatants and non-combatants, violence and non-violence (especially in cyberspace) becomes difficult to achieve. The advanced technological products can easily substitute in-theater forces deployments. For example, an unmanned air vehicle can neutralize a target so that the enemy would not even realize who the attacker is or what hit him. *The combination of commercial autonomous systems with various other easy to procure harmful products (e.g. chemical and biological) feeds the autonomy of the criminal individuals or groupings*. There is, therefore, a high risk of such "weapons" being irrationally operated by various insurgent forces[8], like terrorist organizations and paramilitary forces in destabilizing criminal actions.

The unprecedented development of the Internet and the access to intelligent mobile devices define not only *what we do but also what we are*. Our private life and own needs (translated into consumption indicators), leisure, traveling itineraries, social activity are just some features that define us as individuals and that no longer belong exclusively to us due to the development of the new smart applications. Social technologies multiply the force of ideas expressed by small groups of individuals or social movements which become capable of significantly influencing the behavior of the communities and states they are part of.

3.2. The geographical shift of the global economic power

Recent studies indicate a trend of rebalancing economies globally[9]. Western economic domination is threatened by progressive economic growth in Central and Southeast Asia. Developing countries in these specific regions will be more willing to invest in defense and security, and to develop their autonomy at regional level, possibly by (re)evaluating alliances with great powers (e.g. US, Russia, China). In the long run, population aging in developed regions (like Europe) generates an economical shift worldwide. This makes possible the distribution of economic growth from Europe to the underdeveloped regions in Asia and Africa, where the demand for basic resources like food, water and energy[10] will proportionally increase with the number of people[11]. In this scenario, competition for the access to these resources will grow, both within and between states, leading in extreme cases to conflicts and war.

3.3. Poor / good governance

States, from the most advanced ones to the emerging economies, face challenges in ensuring the political, economic, legal and social

[6] Klaus Schwab, "*The Fourth Industrial Revolution - What It Means and How to Respond*", available on https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution, accessed on 20.05.2017.

[7] *Ibidem*.

[8] Independent Commission on Multilateralism, International Peace Institute, *Discussion Paper - The Impact of New Technologies on Peace, Security, and Development*, April 2016, p. 10, available on https://www.icm2016.org/IMG/pdf/new_tech_paper.pdf, accessed on 11.10.2017.

[9] PrincewaterhouseCooper (PwC), *The World in 2050 - The long view: how will the global economic order change by 2050?*, available on http://www.pwc.com/gx/en/issues/economy/the-world-in-2050.html, accessed on 22.05.2017.

[10] Food and Agriculture Organization (FAO) estimates an increase of 70% in total food request by 2050. The Organization for Economic Co-operation and Development (OECD) estimates that global water demand will increase by 55% by 2050.

[11] The latest UN report (published in 2015) on "World Population Prospects" indicates an average increase in the world population of about 83 million people each year. The forecasts set in 2015 predict that the human population will continue to grow to about 8 billion people in 2024 and 9 billion in 2040. The report is available on https://esa.un.org/unpd/wpp/Publications/Files/Key_Findings_WPP_2015.pdf, accessed on 21.05.2017.

framework contributing to the development of their own societies. Progress and stability of the societies are limited by the spread of corruption, lack of decision-making transparency and deviations from human rights. These phenomena lead to an increase in the gaps between civil society and authorities and, as a consequence, the vulnerability of the latter to shocks[12].

4. The emergence of hybrid patterns in the global security environment

4.1. Non-state actors conduct

The empty space created by the collapse of the failed Third World countries has led to the emergence and perpetuation of regional security crises with global implications. The recent actions of the terrorist groups in the Middle East and North Africa conflicts, as well as in the Western European states[13] reflect *the hybrid and complex nature of the current terrorist phenomenon*. The potential of terrorist groups is rising globally. The line between the in-theater actions and the outside operations on the Western soil (like the latest attacks conducted in Europe) becomes more and more blurred. ISIS activity in Middle East reveals a new center-periphery approach in terrorist actions. ISIS has concentrated its strength *inside the theater of operations* and attempted to capitalize its operational success *outside the controlled areas* across the entire Muslim world by seeking to spread the radical ideology and to attract new operatives for the forthcoming terrorist attacks. ISIS actions proved to get a high global influence, primarily because of the high adherence by its sympathizers to the ideology of Islamic radicalism. We say thus a new form of *domestic terrorism* is born, in which the threats prevails from the internal radicalized elements.

Unlike terrorist groups, whose operational pattern is limited to deliberately escalating the level of violence in their areas of operations and interest, a clear distinction between militias, local insurgent groups and paramilitary formations is difficult to achieve, considering the use of violence criteria. The conflict in eastern Ukraine revealed a pattern of complex insurgency. Local militias emerged as an important player in the conflict based on their Russian ethnolinguistic affiliation which played a central role in destabilizing Donbass and afterwards taking control of it by instating a pro-Russian parallel administration and paramilitary forces. It is proven that local insurgency reproduce and rely on certain indigenous factors that make the host nation vulnerable. However, the paramilitary forces arise mainly in an advanced form of separatism with the political and logistical support of a sponsoring state.

4.2. State actors conduct

The neoliberal influences and rules governing the IR, such as the international humanitarian law that regulates the armed conflicts continue to reduce the risk of a classical war between actors, but do not completely eliminate it. However, a new global war (in its historical connotation) is difficult to imagine at the moment *when the military component is mainly a disincentive instrument*. In this context, *confrontation is more likely to take place at the regional level, within the great powers' areas of interests, without escalating into an extensive and intense armed conflict*. Recent developments reveal three types of "revisionist tactics" that are used by the emergent great powers to achieve competitive advantage at the regional level: avoiding opponent's "red lines", using proxies as aggressors, and facing the opponent with *fait acompli* type situations[14].

- ***China's actions in the East China Sea and the South China Sea***

China's and Taiwan's claims on the Senkaku / Diaoyu archipelago in the East China Sea (which is under the control of Japan) became evident after the findings in 1968 of some new oil resources

[12] *Global trends - Paradox of Progress*, National Intelligence Council, 2017January, NIC 2017-001, p. 67, available on www.dni.gov/nic/globaltrends, accessed on 22.05.2017.

[13] See the attacks in Europe starting with 2015 (in France, UK, Germany and Spain).

[14] Van Jackson, *Tactics of strategic competition - Gray Zones, Redlines, and Conflicts before War*, Naval War College Review, Summer 2017, Vol. 70, No. 3, available on https://search.proquest.com/openview /38ffba5bf77fcfbcb87a9cdac1f5b1a3/1?pq-origsite=gscholar&cbl=34989, accessed on 03.06.2017.

in the area. According to data released by the Coast Guard of Japan[15], China has increased the presence of its civilian and military ships nearby the Japanese islands since 2012. Chinese navy operations have been complemented by aviation. Most of these actions meant to test the "red lines" and reactions of Japan. It should be noted that these actions were directed without the escalation of violence. China's establishment in November 2013 of an *"air defense identification zone"* in the East China Sea, including the Japanese islands, has been an attempt to change the *status quo* in the region and take control of the islands by intimidating Japan.

Starting in 2013, China has engaged in a rapid process of *artificially rebuilding the reefs from Spratly archipelago* in the South China Sea (claimed by China, the Philippines, Taiwan, Vietnam and Brunei). Later on, in 2016, China switched to the militarization of the Fiery Cross, Mischief and Subi artificial islands by building military infrastructure and facilities there[16]. Through these actions, China seeks the expansion of its Exclusive Economic Zone and the control over the shipping lines of energy in Southeast Asia. The artificial construction of the islands in the Spratly archipelago is a *fait accompli* situation for the other states disputing the control of the islands and also for the US by attempting to limit the freedom of movement of its naval vessels in the region and expanding control over one of the major maritime trade routes from Southeast Asia.

- ***Russia's approach in Georgia and Ukraine***

In 2008, Russia engaged in an open conflict with Georgia. The escalation phase lasted only five days. During the confrontation, Russia combined conventional military forces with local guerrilla groups and information operations[17]. The strategic objectives of Russia were to protect the pro-Russian separatists in South Ossetia and Abkhazia and to deter Georgia to join NATO[18]. Russian action was also a warning message to the states aspiring to join NATO (e.g. Ukraine) or to enhance their relation with the Alliance (the case of the Republic of Moldova) and a firm reaction to the "open door" policy endorsed by NATO and EU in Eastern Europe and Caucasus.

The annexation of Crimea Peninsula to Russia (2014) undoubtedly represented a turning point in the Russian-Western relations, a *fait accompli* to Ukraine. It was actually the moment which indicated the return of Moscow's assertive behavior regarding the US and its European allies. In fact what was surprising in Ukraine was the *modus operandi* applied in both the annexation of Crimea and the destabilization in Donbass region. Unlike in Georgia, in Ukraine the military forces were not used overtly due to the limitations imposed by the conditions in the operational environment and the political consequences generated by such a course of action. What emerged, instead, was the principle of the adaptive use of the military force, introduced by the Chief of the General Staff of the Russian Armed Forces, Valeri Gerasimov[19] and the widespread engagement of subversive informational operations (like propaganda and disinformation) targeting both the Ukrainian population and the international public opinion.

The implications of these conflicts are beyond the regional security context. We can easily observe that these diffuse actions were initiated by great powers in different areas of competing interests with the US and some other regional actors.

5. Emerging conflicts' driven threats

5.1. The hybrid image of warfare in the new international system

War is undoubtedly a phenomenon that generates change in the international system. Carl von Clausewitz rightly stated that "every age has

[15] Available online http://www.mofa.go.jp/region/page23e_000021.html, accessed on 03.06.2017.

[16] Asia Maritime Transparency Initiative, available online https://amti.csis.org/chinas-sam-shelters-spratlys/, accessed on 03.11.2017.

[17] Nathan P. Freier (editor), *Outplayed: regaining strategic initiative in the gray zone*, Strategic Studies Institute, available online https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1325, accessed on 12.09.2017.

[18] *Ibidem.*

[19] Valeri Gherasimov, *The Value of Science is in the Foresight*, (translated) Military Review, January - February 2016, available online http://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/January-February-2016/, accessed on 22.02.2017.

its own type of war, its own limited conditions, and its own peculiar preconceptions"[20]. In our opinion, the post-modern conflicts are a product of the neoclausewitzian theory of warfare with all the idiosyncrasies that arise from it:

- *War, as a form of violence escalation, remains an instrument of politics*. In other words, policy determines the opportunity and the intensity of the military force in confrontation. The future confrontation tends to be more political than military and to take place in the areas of interests of the various competing actors. The rise of political competition among the great actors becomes possible if the military factor serves as a deterrence instrument and the opposing great actors prefer to annihilate their adversaries by using "soft" power instruments avoiding therefore the high political and economic costs posed by the military option. Nowadays *alternative cooperation formats* are established in order to solve the recent security crises[21] by excluding US participation. This signs the decline of the UN authority and the Western global liberal influence (represented by the US and the European states) and the reinitiating of political competition among the great actors with competing interests at regional and global level (US, China and Russia).
- *Hybrid warfare does not bring novelty or significant changes in the nature of the warfare, but in its character.* Essentially, Clausewitz's "remarkable trinity", interpreted as the relationship between the three factors that influence the way of conducting warfare - political, military and social - also applies to current conflicts.
- *Hybrid warfare is not only an option of states but also of individuals and non-state actors*. The three elements invoked by Clausewitz in his trinity are also found in the latest forms of insurgency or terrorist actions. Thus, their *reason* (policy) is reflected in the aspirations and attempts to establish a pseudo-state or a cross border type of terrorist organization (in the most recent ISIS case). *Violence* is fed by the radical ideological trends promoted among the targeted population (emotion) and, finally, the *uncertainty* (chance) can be found in the victory (which is always questionable) against the opponent.
- Even though the military element is not the dominant one, *hybrid warfare remains "an act of violence in order to force our opponent to fulfill our will"[22], only that aggression and violence manifest themselves in the cognitive and informational domains*. The violence of pseudo-organized masses revealed in social protest and / or the passive form of violence which is increasingly visible online overlap on the classical violence caused by, or in conjunction with, military force. Connecting the dots between these types of violence may be essential in achieving success within hybrid scenarios of postmodern warfare.
- *The declining role of the classical military factor in postmodern conflicts makes it difficult to clearly separate peace from war.* Military aggression is an attribute of war. However, it only performs in a higher stage which can be associated with the transition of the conflict in crisis, while informational aggression, coercive diplomacy and cyber-attacks, for example, can manifest in the whole spectrum of confrontation, in peacetime, tension/conflict, crisis and war.
- *Energy steering in order to annihilate the opponents' centers of gravity is also preserved in hybrid scenarios only that in the latter case the energy focuses on vulnerabilities.*

5.2. The conceptual model of the threat in hybrid confrontation scenarios

Russian *modus operandi* in Ukraine cannot identically apply on another target because simply the operational environment conditions are not alike. We should avoid to become biased and wrongly chose to prepare fighting past wars. For a better understanding of the particularities of the emerging conflicts, we consider useful and appropriate the effort to conceptualize the threats derived from the actual diffuse and hybrid confrontations (Figure no.1). In our opinion, the threats in the new hybrid confrontation scenarios

[20] Carl Von Clausewitz, *On War*, Princeton, NJ: Princeton University Press, 1976, p. 240.

[21] The Minsk talks to resolve the crisis in Ukraine, the Astana negotiations on the regulation of the Syrian conflict and the possible revitalization of negotiations in the Six Group on the North Korean nuclear dossier.

[22] Carl von Clausewitz, *op.cit.*, p. 13.

integrate a set of actions / measures undertaken by an aggressor against its target at various possible stages of confrontation.

The *preliminary stage of the confrontation* consists of non-kinetic actions and the use of the political, economic and diplomatic instruments, specific intelligence activities (collection, subversion) and psychological operations (to influence and deter the adversary), military actions planned as a function of active (use of own capabilities in airspace and sea controlled by the opponent) and passive (highlighting the danger of a military intervention or preemptive strikes) deterrence, coordinated by a potential aggressor on its would-be adversary.

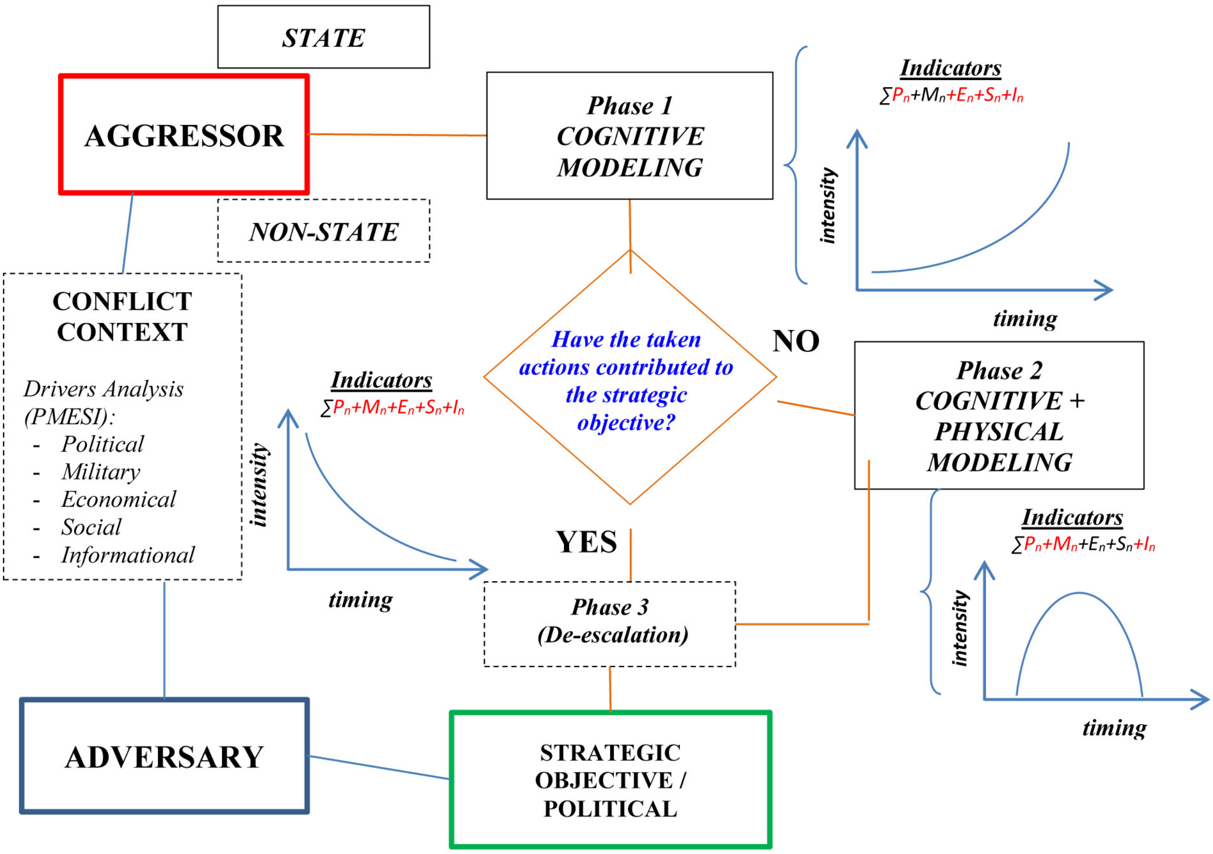


Figure no. 1: Full spectrum threat matrix driven from hybrid confrontations

The use of the armed forces and combat capabilities becomes effective later in *the active phase of the confrontation*. This stage seeks mainly the physical domain of the war (and comprises the measures in the first phase). The new measures may include, as appropriate, establishing anti-access area denial (A2AD) systems, high-precision naval and/or land platforms, support of irregular forces/proxy groups operating on the opponent's territory, and deployment of covert Special Operations forces to neutralize targets placed on the opponent's territory.

The non-kinetic actions (presented in the preliminary stage) and, where appropriate, the deployment of regular military forces under different pretexts (e.g. peacekeeping operations) and, covert, for training the proxy forces are all restored within *the final de-escalation phase*.

Conclusions

The changes in the international system focus primarily on *processes* that shape the relations between actors in different domains of interaction (political, economic, military, social and cultural domains). They maintain a relative balance within the international system. In this context, one cannot speak of a systemic transformation in IR similar to that which determined the post-

World War II bipolarity and the international mechanisms and institutions that contributed later to the normalization of the military conflicts between actors.

The actors' hybrid conduct is determined by the increased geostrategic competition between them and the revisionist tactics of the emerging great powers (such as China and Russia) to legitimize a polycentric international system. Their competing interests impede the international organizations effectiveness in crisis management actions and contribute to the perpetuation and expansion of instability outside the conflict areas (the new security crises retain a global character through the effects generated by the actors involved). This leads to an apparent inefficiency of the international organizations, which seem to be "obsolete", unreformed or incapable of responding to their basic mission, which only exacerbates the tendency of resetting the international order in accordance with the neorealism principles.

Western domination and the "centralized globalization" age is subject to pressure, which is manifested by the rebalancing the inequality of the distribution of the economic development between the "center" ("First World ") and the "periphery" ("Second" and "Third World"). The economic and technological interdependencies that are increasingly evident in international system define "the new globalism", which, however, inclines to be no longer so strongly influenced by a single international actor with "superpower" status. US will certainly remain *primus inter pares* or the actor who will have a big word to say in any problem that sets the international agenda. However, its influence will be challenged by the revisionist actions of its competitors both in the Western "core", amid the challenges that make fragile the transatlantic relation, and in the "periphery". This trend is merely the expression of the geostrategic competition and the emergence of regional security complexes. Thus, the competing actors behavior integrates a set of *legal and illegal instruments* and *conventional and unconventional means* to express power, widely used, *at the boundary between peace and war*. Actors challenging the current world order will identify those means in the "gray zone" (political, economic, social, military, etc.) whose combination and timing will contribute to gaining competitive advantage or securing stakes in controlling disputed areas. The disputed areas are not necessarily territories (although the case of Crimea or Chinese artificial islands in the Spratly archipelago confirms this hypothesis), but especially political, economic and informational domains of interaction.

Increasing the global relevance of non-state insurgency with the sponsor nations' support remains a multiplier of complexity in the global security environment. Their role will grow as geostrategic competition amongst state actors will also increase. The involvement of various paramilitary groups and local militias in conflicts on the part and with the sponsor nation support highlights a relative level of insurgency's autonomy at regional level (Ukraine, Yemen, Syria, and Iraq).

The separation between the different states that can characterize the relations between actors - *peace, crisis, conflict or war* - will be difficult to achieve as long as the actors remain committed to avoid escalating violence. *Hybridity subsists in all of the four previously described states. What is different in each of them is the nature of the consequences generated through the aggressor's strategy of combining the different methods and instruments it retain*. The distinction between peace and war is increasingly difficult to achieve also because, in many cases, relations between the parties go beyond *physical confrontation* (where classic military operations are taking place). These are taking place predominantly in the *cognitive* (in which knowledge assures the implementation of the strategic decision) and *informational realms* (in which information is created and manipulated), where the consequences of the aggressor's actions can be difficult to identify from its victim due to its misperception the general state of confusion that emerges.

Avoiding escalation of violence and a large-scale armed conflict is common sense for the revisionist great powers. However, this emphasizes the political side of IR (especially those conducted with the dominant power in the international system). A multipolar international system may increase the risk of armed confrontation (although not a large-scale one) between actors in regions where their interests are divergent and interfere. Transforming into the international system is not a matter of today, but a constant that requires a permanent capacity for adaptation by actors, especially those without a high regional influence but who are positioned at the confluence of the interests of great powers and face multiple security challenges.

BIBLIOGRAPHY:

1. BUZAN, Barry, *New Patterns of Global Security in the Twenty-First Century*, International Affairs (Royal Institute of International Affairs 1944-), Vol. 67, No. 3 (Jul.,1991), p. 437, available: http://www.jstor.org/stable/2621945.

2. CLAUSEWITZ, Carl Von, *On War*, Princeton, NJ: Princeton University Press, 1976.

3. GHERASIMOV, Valeri, *The Value of Science is in the Foresight*, (translated) Military Review, January-february 2016, available: http://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/January-February-2016/.

4. GORDEEVA, Evgenia, *Transforming international system and the three approaches to the security dilemma, European Journal of Futures Research*, Volume 4, available: https://link.springer.com/article/10.1007/s40309-016-0088-y.

5. HOFMANN, Frank. G., *Hybrid wars and challenges*, JFQ / issue 52, 1st quarter 2009, available: www.ndupress.ndu.edu.

6. KEOHANE, Robert, *After Hegemony: Cooperation and Discord in the World Political Economy*, Princeton University Press, 1984.

7. KANT, Immanuel, *Toward Perpetual Peace and other writings on politics, peace and history: a philosophical essay*, Yale University Press, 2006.

8. SCHWAB, Klaus, *The Fourth Industrial Revolution - What It Means and How to Respond*, available: https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution.

9. JACKSON, Van, *Tactics of strategic competition - Gray Zones, Redlines, and Conflicts before War*, Naval War College Review, 2017, available: https://search.proquest.com/openview/38ffba5bf77fcfbcb87a9cdac1f5b1a3/1?pq-origsite=gscholar&cbl=34989.

10. FREIER, Nathan P. (editor), *Outplayed: regaining strategic initiative in the gray zone*, Strategic Studies Institute, available: https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1325.

11. ***, *Global trends - Paradox of Progress*, National Intelligence Council, 2017, NIC 2017-001, p. 67, available: www.dni.gov/nic/globaltrends.

12. ***, Independent Commission on Multilateralism, International Peace Institute, *Discussion Paper - The Impact of New Technologies on Peace, Security, and Development*, aprilie 2016, available: https://www.icm2016.org/IMG/pdf/new_tech_paper.pdf.

13. ***, Princewaterhouse Cooper (PwC), *The World in 2050 - The long view: how will the global economic order change by 2050?*, available: http://www.pwc.com/gx/en/issues/economy/the-world-in-2050.html.

14. ***, *Perspectivele Populației Mondiale,* raport al ONU, 2015, available: https://esa.un.org/unpd/wpp/Publications/Files/Key_Findings_WPP_2015.pdf.

15. ***, *SIPRI Military Expenditure Database*, Stockholm International Peace Research Institute, available: https://www.sipri.org/databases/milex.

16. ***, *European Union Global Strategy*, 2016, available: eeas.europa.eu/archives/docs/top.../eugs_review_web.pdf.

17. ***, *World Economic Outlook (October 2017)*, International Monetary Fund, available: http://www.imf.org/external/datamapper/NGDP_RPCH@WEO/OEMDC/WEOWORLD/CHN/USA/ADVEC/EU/AS5/DA/BRA/IND.

BAHRAIN'S ROLE IN THE GEOSTRATEGIC VISION OF IRAN AND SAUDI ARABIA

*Răzvan MUNTEANU**

Even though, subsequent to the Islamic Revolution in Iran in 1979, Riyadh and Tehran entered into a geopolitical competition for supremacy in the Muslim world, the two states were strategic partners sharing core interests, such as fighting the spread of Communist ideology and of pan-Arabism. Despite this, both before and after 1979, the state of Bahrain, made up of 33 isles, of which only two are inhabited, has represented a cause for dispute between Saudi and Iranian interests.

This article proposes to highlight the strategic importance of Bahrain to both Iran and Saudi Arabia, in the context of their geopolitical rivalry, especially since Bahrain is a majority Shiite state ruled by a Sunni minority. Starting in 1979, the Shiites of Bahrain have been emboldened by the Islamic Revolution to demand new rights, such as accession into upper governmental positions, but their marginalization continued under a policy of Manama supported by Riyadh. Thus, Bahrain became the field for a proxy conflict between Saudi Arabia and its allies in the Sunni monarchy of the state and Iran, whose strategy has been to support non-state actors to destabilize Bahrain in order for Shiites to assume power. Such a scenario is, however, viewed by the Saudis as a threat to their national security and to the regional status quo.

***Keywords**: geopolitics, Bahrain, the Persian Gulf, Saudi Arabia, Iran, Arab Spring, proxy war.*

Introduction

With a population of 1,410,942 inhabitants[1], the tiny state of Bahrain is an important geostrategic linchpin for the balance of power in the Persian Gulf in the context of the current geopolitical competition between Saudi Arabia and Iran.

The archipelago is made up of 33 islands, of which only two are habitable, and was occupied by the Portuguese in the period between 1522-1602, after which it entered Arab and then Persian possession[2]. The influence of Iran in Bahrain starts in 1602, during the Safavid Dynasty and lasts until 1782, when the military expansion of the Sunni al-Khalifa tribe takes place. The regional Shiite population migrates to the North and West of the area under the pressures of these developments, where they remain to this day[3]. The al-Khalifa, hailing from the Qatari peninsula, have ruled Bahrain until the present day, utilizing

[1] ***, "Bahrain", CIA The World FactBook, available at https://www.cia.gov/library/publications/the-world-factbook/geos/ba.html, accesed on 01.06.2017.

[2] ***, "The Strategic Importance of Bahrain to Saudi Arabia", in *The Oil Price*, 29.07.2011, available at http://oilprice.com/Geopolitics/Middle-East/The-Strategic-Importance-Of-Bahrain-To-Saudi-Arabia.html, accesed on 03.06.2017.

[3] Jason Rivera, "Iran's Involvement in Bahrain: A Battleground as Part of the Islamic Regime's Larger Existential Conflict", in *Small Wars Journal*, available at http://smallwarsjournal.com/printpdf/22533, accesed on 01.06.2017.

Răzvan MUNTEANU is PhD. Researcher in Political Science at National School for Political Science and Public Administration, Bucharest, Romania. E-mail:razvan.munteanu@newsint.ro; r.munteanu88@yahoo.com

the backing of the British, who turned the country into a protectorate in 1830[4], as well as that of the Americans, who assumed the role of the British in the region in the wake of the discovery of the Persian Gulf energy reserves.

Although the American presence in the region dates back to 1948, the first military accord between the two countries was signed in 1971, with the US Navy receiving access to Port Salman starting in 1977. In 1995, the US 5th fleet moved its headquarters to Bahrain[5] to maintain the status quo and the regional security architecture.

Between the diminishment of the British role in the region and the arrival of the Americans, both Iran and Saudi Arabia claimed the archipelago as their respective territory, which led to a UN mandate which eventually decided in favor of awarding Bahrain its independence under the rule of the al-Khalifa family[6]. With its roots in the House of Saud, the al-Khalifas have maintained a close relationship with Saudi Arabia, which brought the state into its sphere, despite the majority religion of the population.

Beyond the common historical and ideological roots of the two dynasties, ties between the two countries were also consolidated through the marriage of the son of King Abdullah to the daughter of King Hamad al-Khalifa[7].

All this time, the Shiites have remained a marginalized community, its members unable to take on high level political roles, while the government practices a policy of giving citizenship to Sunni Arab expats in order to modify the demographic balance[8]. This has been a source of growing social tensions and deepening sectarian rifts.

While the Shiite population of Bahrain is divided into two main branches – the *Baharna* for those of Arab origin and the *Howala or 'Ajams*, for those with Persian roots – in practice it has been in close contact with Iran and faithful to the regime in Tehran[9], which is due, most likely, to the policies of marginalization to which the Shiites were subjected in Bahrain as far back as during Ottoman rule, with the calls for rights appearing after the 1979 Islamic Revolution[10]. It was that event which made the Saudi Government accelerate the construction of the bridge and highway system called the *King Fahd Causeway*, which ties Saudi Arabia to Bahrain[11].

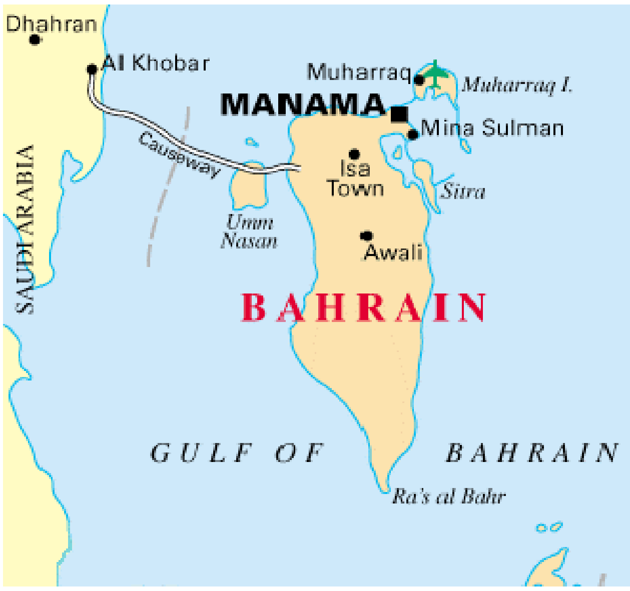


Figure no. 1: King Fahd Causeway

Source: Al Arabiya, https://english.alarabiya.net/, accesed on 28.05.2017

Finalized in 1986, the King Fahd Causeway is presented as a project meant to enhance economic relations between the two countries, but, in reality, represents also a military infrastructure to allow the Saudi Armed Forces to rapidly deploy in Bahrain[12], a role which was highlighted during

[4] "The Strategic Importance...", *op. cit.*

[5] Delshad Khezri, "The Islamic Awakening in Bahrain and Geopolitical Developments in Persian Gulf", in *Indian Journal of Scientific Research*, 1/ 2014, pp. 300-306.

[6] Simon Mabon, "The Battle for Bahrain: Iranian-Saudi Rivalry", in *Middle East Political Council*, Volume XIX, Summer, Number 2, available at http://www.mepc.org/battle-bahrain-iranian-saudi-rivalry, accesed on 02.05.2017.

[7] *Idem.*

[8] *Ibidem.*

[9] Jacques Neriah, "Iranian-Saudi Tensions Are Played Out in Bahrain", in Institute for Contemporary Affairs, Vol. 17, No. 1, available at http://jcpa.org/article/iranian-saudi-tensions-played-bahrain/, accesed on 01.05.2017.

[10] Jason Rivera, *op. cit.*

[11] Simon Mabon, *op. cit.*

[12] *Ibidem.*

the Arab Spring, when Saudi troops and UAE special forces entered Bahrain to reinforce the al-Khalifa regime against Shiite protesters.

Even while the oil reserves of Bahrain are nearly depleted[13], influence over this state is a cause for dispute between Iran and Saudi Arabia. This paper sets out to prove the strategic importance of Bahrain in the context of Iranian-Saudi geopolitical rivalry, as well as the reasoning behind Manama's stance towards the states in region.

1. Proxy rivalry

The Iranian involvement in Bahrain takes place indirectly, through proxy actors, as well as directly, through messages of support for certain Shiite leaders and through the continuing messages containing territorial claims on the islands.

For instance, in 2007, the Iranian newspaper Kayhan, well known for its proximity to the Supreme Leader in Tehran, published an article where it was mentioned that, pursuant to "incontestable documents", Bahrain had been "Iranian territory up until 26 years ago". Two years later, the former President of the Majlis (the Iranian Parliament), Akbar Nateq Nuri, declared that "Bahrain had been the fourteenth province of Iran until 1970"[14].

In essence, the Islamic Revolution was an awakening of the Shiite community and also promoted its organization into political parties and the attempt to play an important role in the state structures of the nations where they are located[15]. This is why, after 1979, Iran supported the creation of non-state actors to foment revolutionary movements in Bahrain, including through the use of terrorist action[16].

Two years later, in 1981, Manama accused the Islamic Front for the Liberation of Bahrain (IFLB)[17] of attempting to orchestrate a coup.

The IFLB had been created in the mid-1970s to install a theocratic regime in Bahrain. One of its leaders, Hadi al-Modarresi, publicly affirmed that he wished to import the Islamic Revolution[18] and studies have shown that the group was influenced by Iran through ideology, leadership, as well as media, logistic and military support[19]. Another example of Iranian proxy action to destabilize the Sunni regime in Bahrain is the creation and financing of the group Hezbollah al-Hejah, which was supposed to be a copy in the Gulf region of the Lebanese Hezbollah, specifically intended to destabilize the regimes of Saudi Arabia, Kuwait and Bahrain[20].

In 2013, another Shiite paramilitary group was born in Bahrain, titled Saraya al-Mukhtar, after an important Shiite historical figure and utilizing a logo similar to that of the Iranian Revolutionary Guard. While it mostly delivers online propaganda, it has been involved in skirmishes with law enforcement[21]. On September 25th, 2013, Muhammad Abdul Ghaffar, the Bahraini Royal Advisor for diplomatic affairs accused Iran in no uncertain terms during a UN Summit: "The kingdom of Bahrain has been suffering for a long time from the Iranian interference in its internal affairs. There are multiple TV channels that are under Iranian influence, along with a number of radio stations, newspapers and media institutions that are affiliated with Iran."[22].

[13] Simon Henderson, "Saudi Arabia's Fears for Bahrain", in The Washington Institute, Policy Analysis, February 17, 2011, available at http://www.washingtoninstitute.org/policy-analysis/view/saudi-arabias-fears-for-bahrain, accesed on 28.05.2017.

[14] Simon Mabon, *op. cit.*

[15] Delshad Khezri, *op. cit.*

[16] Jason Rivera, *op.cit.*

[17] IFLB is at the same time known in the arab world as *Al-Jabha al-Islamiyya li Tahrir al-Bahrayn.*

[18] Kevin Downs, "A Theoretical Analysis of the Saudi-Iranian Rivalry in Bahrain", in *Journal of Politics & International Studies*, Vol. 8, Winter 2012/13, p. 214.

[19] Simon Mabon, *op. cit.*

[20] Jason Rivera, *op. cit.*

[21] Abbas Qaidaari, "Does Iran have a card to play in Bahrain?", in *Al Monitor*, march 17, 2015, available at http://www.al-monitor.com/pulse/originals/2015/03/iran-bahrain-saraya-mukhtar.html#ixzz4sZVXwmlX, accesed on 09.06.2017.

[22] Muhammad Abdul Ghaffar, apud Yasser al-Chazli, (2013) "Adviser to Bahrain king: GCC basis of balance in region," *Al-Monitor*, http://www.al-monitor.com/pulse/tr/security/2013/11/bahrain-gcc-balance-unrest-iran.html# apud Jason Rivera, *op. cit.*

Despite this, the climax of the Saudi-Iranian rivalry over Bahrain was reached during the Arab Spring, when over 200,000 Shiites[23] took to the streets of major cities to protest against the al-Khalifa family. The Saudis sent financial aid to Manama to institute social policies, as well as 1,200 soldiers, with another 800 special forces troops from the United Arab Emirates, who traversed the King Fahd Causeway and violently repressed the anti-regime manifestations in Bahrain[24]. While there was a strong discourse on both sides, with Saudi Arabia and Bahrain accusing Iran of supporting the protests and interfering in the internal affairs of another state, and Iran advocating for the rights of the Shiites in Bahrain, only one side sent troops to the region. Iran refrained from sending military personnel to Bahrain, showing that it prefers proxy conflicts to achieve its strategic objectives, while a military confrontation with Saudi Arabia and especially the United States, which has its own military presence in the archipelago, is a red line that cannot be crossed.

Evidently, tensions between Bahrain and Iran are far from subsiding, and not even the signing of the Joint Comprehensive Plan of Action between Tehran and the P5+1 and the EU did not dampen these tensions.

One example is the announcement made by the government in Manama on July 25th, 2015, a week after the signing of the JCPOA, that it had found a smuggling operation for Iranian weaponry, as well as a clandestine explosives factory[25]. Also in 2015, the US released a report in which it is stated that Iran "provided weapons, funding, and training to Shia militants in Bahrain"[26].

That same year, as the Bahraini rulers celebrated four years since the Saudi military intervention, the Shiites organized meetings in Manama and Sitra, where they chanted slogans such as "We are all members of the resistance" which, in Middle Eastern terms, translates into support for opposition movements in the Iranian sphere of influence, such as Hamas or Hezbollah[27].

2. Bahrain's geostrategic importance

The escalating social tensions arise from the marginalization and discrimination of the Shiite community in Bahrain, a policy which Saudi Arabia practices towards its own Shiite community, numbering 10-15% of the total population[28]. Both Saudi Arabia and Bahrain view their Shiites as a possible Iranian 5th column[29], stoking mistrust and justifying the denial of political and social rights to the Shiites.

The Shiite population in Saudi Arabia is found in the Eastern province, close to Bahrain (see figure no. 2), where a possible emancipation of the Shiites in the neighboring state or their assumption of power through revolutionary

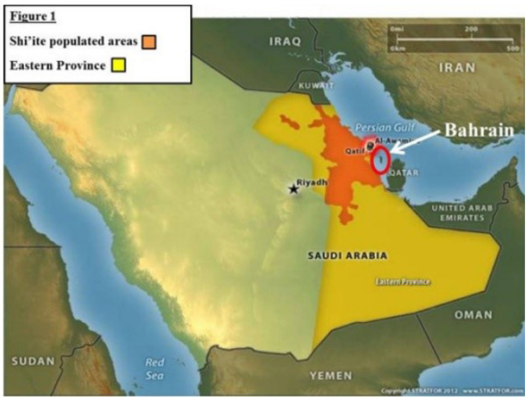


Figure no. 2: The Shiite population in Saudi Arabia and the proximity to Bahrain

Source: *Oil Price, http://oilprice.com/*, accesed on 28.05.2017.

[23] Tali Rachel Grumet, "New Middle East Cold War: Saudi Arabia and Iran 's Rivalry", University of Denver, available at http://digitalcommons.du.edu/cgi/viewcontent.cgi?article=2027&context=etd, accesed on 01.05.2017.

[24] René Rieger, "In Search of Stability: Saudi Arabia and the Arab Spring", Gulf Research Center, 2014, available at https://www.files.ethz.ch/isn/182104/GRM_Rieger_final__09-07-14_3405.pdf, accesed on 07.02.2017, p. 6.

[25] Tzvi Kahn, "Iran's Proxy War in Bahrain", in The Foreign Policy Initiative, availble at http://www.foreignpolicyi.org/content/fpi-bulletin-iran%E2%80%99s-proxy-war-bahrain, accesed on 18.05.2017.

[26] *Ibidem.*

[27] Abbas Qaidaari, *op. cit.*

[28] CIA factbook.

[29] Laurence Louër, "Sectarianism and Coup-Proofing Strategies in Bahrain", in *Journal of Strategic Studies*, 36:2, p. 246.

means would embolden the local Shiite community towards rebellion or even secession. Thus, Riyadh perceives such events in Bahrain as an implicit threat to its own territorial integrity.

The entry of Bahrain into the Iranian sphere of influence would lead either to a withdrawal of the United States from the region, or to an Iranian-American alliance which would impact Saudi interests, moreso since the US has been a deciding factor since 1979 in limiting Iranian influence in the GCC Member States (Saudi Arabia, Bahrain, Oman, Kuwait, Qatar and the United Arab Emirates) and in Shiite communities in these countries.

The proximity of the two countries places Bahrain approximately 20 kilometers away from Saudi critical oil infrastructure, as can be surmised from Figure no. 3. This infrastructure is made up of:

- Oil fields: Ghawar, Abqaiq, Abu Safah, Qatif, and Berri;
- Oil export terminals: Ras Tanura, Al Juaymah;
- Water processing facilities in Abqaiq;
- Water treatment facilities in Qurayyah[30].

Saudi vulnerabilities are amplified by the location of the oil infrastructure in its Eastern Province, a Shiite area which could be mobilized by Iran for a conventional or non-conventional conflict, through guerilla operations or terrorism.

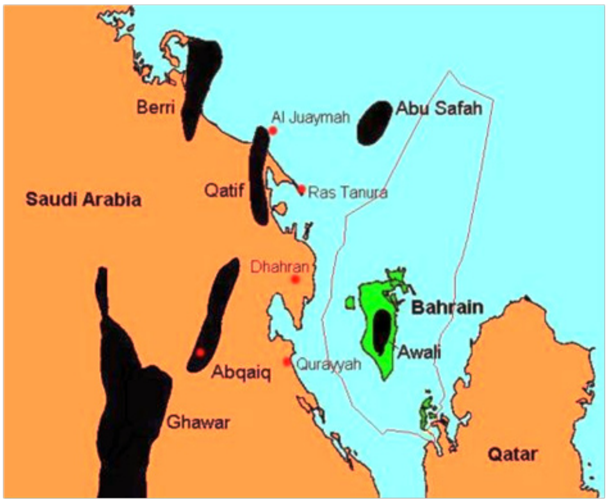


Figure no. 3: Saudi critical infrastructures and their proximity to Bahrain

Source: *Oil Price, http://oilprice.com/*, accesed on 28.05.2017.

While Saudi Arabia is, culturally, the most conservative Arab state, Bahrain is much more liberal, which offers a pressure valve for Saudis crossing the King Fahd Causeway to consume alcohol, eat pork or enjoy the nightlife[31].

For Iran, the control of the Gulf routes is perceived as a national security priority, which is why Tehran has been uncomfortable throughout its history with any foreign presence in the Persian Gulf, whether British or America[32]. Finally, the installation of a favorable regime for Tehran in Bahrain would legitimize Iranian policies in the region and offer Iran significant power projection capabilities, aiding it in becoming a regional hegemon with influence over the oil policies of the Persian Gulf riparian countries, which is the richest region in fossil fuels in the world.

Final considerations

Bahrain is a strategic and military buffer area separating Saudi Arabia from Iran and serving a fundamental role in the security architecture of the Persian Gulf. Any step towards instability in this country is a vulnerability for Riyadh and an opportunity for Tehran which could lead to a change in the regional status quo.

The Iranian strategy hinges on the cultural factor, where the Bahraini Shiite community is influenced towards its own ends, as well as the historical factor, by reinterpreting the past to advance irredentist claims over the Archipelago, thereby penetrating the Gulf Security Council, weakening Saudi Arabia and obtaining regional hegemony.

For the Saudis, the events in Bahrain are considered to directly endanger national security, especially since Riyadh sees the Gulf Shiite communities as a tool of Tehran to destabilize the

[30] *"The Strategic Importance..."*, *op. cit.*

[31] Simon Mabon, *op. cit.*

[32] Sina Azodi, "Iran, the US, and the Persian Gulf", in *The Diplomat*, 05.11. 2016, available at http://thediplomat.com/2016/11/iran-the-us-and-the-persian-gulf/, accesed on 08.05.2017.

Monarchies, which would lead to the import into Saudi Arabia of the Bahraini sectarian cleavage possibly resulting in the break-up of Saudi Arabia.

Therefore, Bahrain is a theater for proxy warfare, where the Saudis offer military and financial support to the Manama regime led by the al-Khalifa family, while the Iranians employ subversive measure to destabilize them. The marginalization of Shiites in Bahrain and Saudi Arabia will continue so long as Riyadh and Manama view these communities with suspicions, and the religious divisions in the Middle East will deepen.

The regional dispute will even fuel divergences regarding the security architecture in the Persian Gulf, where, fearing a possible expansion of Iranian influence, Saudi Arabia will continue to advocate for the presence of a foreign military power, such as the United States, while Iran will endorse a security environment to which only the riparian countries may contribute, rejecting outside influence.

In Bahrain, the political, economic and military power belongs to the Sunni minority, despite numbering 25% of the total population, with the Shiites accounting for the remainder of 75%. This is why the al-Khalifa alliance with Saudi Arabia transcends considerations of history and ideology, and is an alliance necessary for the survival of the monarchy.

BIBLIOGRAPHY:

1. AZODI, Sina, “Iran, the US, and the Persian Gulf”, in *The Diplomat*, 05.11.2016, available at http://thediplomat.com/2016/11/iran-the-us-and-the-persian-gulf/.

2. COATES, Kristian, *Insecure Gulf*, Oxford, Oxford University Press, 2015.

3. DOWNS, Kevin, “A Theoretical Analysis of the Saudi-Iranian Rivalry in Bahrain”, in *Journal of Politics & International Studies*, Vol. 8, Winter 2012/13.

4. GRUMET, Tali Grumet, “New Middle East Cold War: Saudi Arabia and Iran’s Rivalry”, University of Denver, available at http://digitalcommons.du.edu/cgi/viewcontent.cgi?article =2027 &context=etd.

5. HENDERSON, Simon, “Saudi Arabia’s Fears for Bahrain”, in *The Washington Institute*, Policy Analysis, 17 februarie 2011, available at http://www.washingtoninstitute.org/policy-analysis/view/saudi-arabias-fears-for-bahrain.

6. HOURANI, Albert, *Istoria Popoarelor Arabe*, Iaşi, Polirom, 2010.

7. JOYCE, Miriam, *Bahrain from the Twenthieh Century to the Arab Spring*, New York, Palgrave Macmillan, 2012.

8. KAHN, Tzvi, “Iran’a Proxy War in Bahrain”, in *The Foreign Policy Initiative*, available at http://www.foreignpolicyi.org/content/fpi-bulletin-iran%E2%80%99s-proxy-war-bahrain, accessed 18.07.2017.

9. KHEZRI, Khezri, “The Islamic Awakening in Bahrain and Geopolitical Developments in Persian Gulf”, in *Indian Journal of Scientific Research*, 1/2014, pp. 300-306.

10. LEWIS, Bernard, *Istoria Orientului Mijlociu*, Iaşi, Polirom, 2014.

11. LOUËR, Laurence, “Sectarianism and Coup-Proofing Strategies in Bahrain”, in *Journal of Strategic Studies*, 36:2, pp. 245-260.

12. MABON, Simon, “The Battle for Bahrain: Iranian-Saudi Rivalry”, in Middle East Political Council, Volume XIX, Summer, Number 2, available at http://www.mepc.org/battle-bahrain-iranian-saudi-rivalry.

13. NERIAH, Jacques, “Iranian-Saudi Tensions Are Played Out in Bahrain”, Institute for Contemporary Affairs, Vol. 17, No. 1, available at http://jcpa.org/article/iranian-saudi-tensions-played-bahrain/.

14. QAIDAARI, Abbas, “Does Iran have a card to play in Bahrain?”, in *Al Monitor*, 17 March 2015, available at http://www.al-monitor.com/pulse/originals/2015/03/iran-bahrain-saraya-mukhtar.html#ixzz4sZVXwmlX.

15. RIEGER, René, “In Search of Stability: Saudi Arabia and the Arab Spring”, Gulf Research

Center, 2014, available at https://www.files.ethz.ch/isn/182104/GRM_Rieger_final__09-07-14_3405.pdf.

16. RIVIERA, Jason, “Iran’s Involvement in Bahrain: A Battleground as Part of the Islamic Regime’s Larger Existential Conflict”, in Small Wars Journal, available at http://smallwarsjournal.com/printpdf/22533.

17. WEHREY, Frederic ... [et al.], *Saudi-Iranian Relations Since the Fall of Saddam*, RAND Corporation, Report, 2009.

18. ***, “The Strategic Importance of Bahrain to Saudi Arabia”, in *Oil Price*, 29.07.2011, available at http://oilprice.com/Geopolitics/Middle-East/The-Strategic-Importance-Of-Bahrain-To-Saudi-Arabia.html.

THE TOPICALITY OF SECURITY DILEMMA'S SPIRAL MODEL IN ANALYSING THE INTERNATIONAL ENVIRONMENT

Cătălina TODOR*

Although, in the current days, international interdependencies and interconnections are at an unprecedent level - all these phenomena associated with globalization contributing to this state, which has determined the dilution of the space-time representation mostly as a result of the last century evolutions, such as the ones in the field of transport and communications - we do not see an increase in the stability of the international environment, but we are witnessing the emergence of many challenges in understanding its specific dynamics. Therefore, theoretical constructs, such as the one of security dilemma, are extremely useful because they can explain, at least partially, the development of certain types of tense relations between geopolitical actors in the international security environment. Thus, the present research aims to emphasise the topicality of this concept emerged in the 50s and to underline its current usefulness. To achieve this goal, the research is based particularly on the analysis of literature, but also on the statistical data analysis regarding conflict.

***Keywords**: security dilemma, spiral pattern, tension, amplification, attenuation.*

Introduction

The international security environment is becoming more and more difficult to analyse because of its complexity and of the increasing amplitude in some phenomena, such as the diversification of unconventional threats and tensions in relations governed by divergent positions (e.g. the NATO - Russia relation, the US - Russia relation, including position on the "hot" zones - Syria, or on actors with challenging actions - North Korea).

This article aims to briefly and non-exhaustively present the concept of security dilemma as a possible logic that can provide a spiral pattern for analysing the dynamics of the security environment, especially those that concern two actors with divergent positions.

The research starts from explaining the necessity of such a theoretical model and then dedicates a second part to the topicality of the theoretical anchor represented by the "security dilemma", through the most important constitutive elements of the concept. A last part offers a potential methodological framework for developing future case studies by highlighting those constituent elements that a relation between two or more actors must contain in order to fit into the spiral pattern of the security dilemma.

***Cătălina TODOR is Junior Researcher within the Centre for Defence and Security Strategic Studies (CDSSS), "Carol I" National Defence University (ROU NDU), Bucharest, Romania.**
E-mail: todor.catalina@unap.ro*

1. Elements of international context as an analysis object for the spiral pattern of the security dilemma

Recent events outline the year 2017 as a continuation of a period marked by gradual amplification of tensions at regional and global level. Some examples of this might be the tension generated by the difficult relation between NATO and Russia, the US and Russia relation (even during Trump presidential administration), the international community's impossibility to adopt a unitary position in order to ameliorate the situation in conflict zones (e.g. Syria) or bellicose actions specific to some states (e.g. North Korea). On the other hand, the persistence of certain conflict zones or the provocative actions of some countries can serve as geopolitical outlets, highlighting the desire of some actors to show their presence in certain regions or to have a saying in solving regional/global problems.

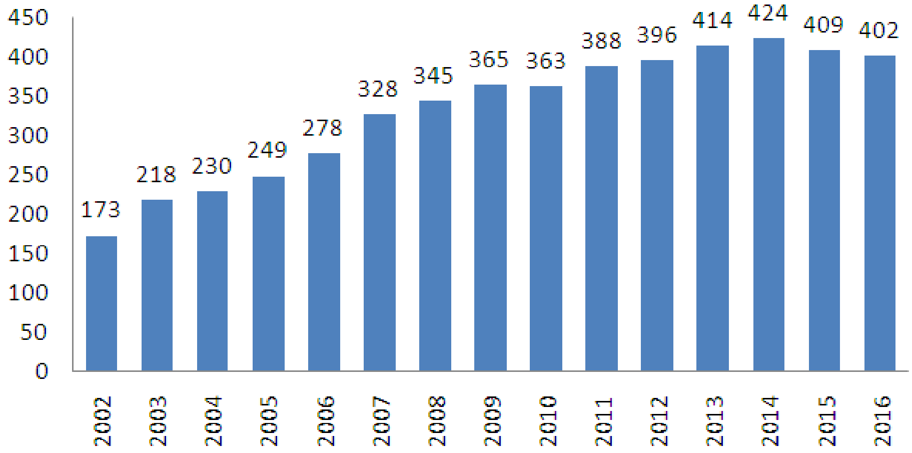


Figure no. 1: Number of conflicts evolution in 2002-2016 period

Sources: The chart is based on the indicator: total number of whorldwide conflicts. This has been selected from each annual report of *Conflict Barometer*; the 15 reports are available online at https://www.hiik.de/en/konfliktbarometer/, accessed on 22.06.2017.

If we study the idea of tension/conflict from a statistical perspective, at global level, the most recent centralized data in this respect are those presented in the *Conflict Barometer 2016*[1].

This barometer provides a classification of conflicts according to five levels of intensity: disputes, non-violent crisis, violent crisis, limited wars and wars, which fall into two main categories: (A) non-violent conflicts: 1. disputes, 2. non-violent crises; (B) violent conflicts: 3. violent crises, 4. limited war, 5. war.

Returning to global tensions, observing the quantitative data, one can notice that over the last few years, the total number of conflicts has generally grown, even though, in particular, we see a slight numerical decrease in 2016. In 2016, there were 402 conflicts, of which 226 were violent and 176 non-violent. In the same year, we see an increase in the following categories of conflict by intensity: the number of disputes increased from 90 to 98 and the number of violent crises raised from 183 to 188. On the other hand, the number of non-violent crises decreased, from 88 to 78, the number of limited wars, from 24 to 20 and the number of wars from 19 to 18.

Analysing the evolution of the total number of worldwide conflicts, from the early years of the publication to date, we find that, although globally, interdependencies and interconnections are at an unprecedented scale and continue to intensify (the dilution of time and space notions as a result of the phenomenon of globalization,

[1] ***, *Conflict Barometer 2016*, Heidelberg Institute for International Conflict, 2017, available online at https://www.hiik.de/en/konfliktbarometer/pdf/ConflictBarometer_2016.pdf, accessed on 07.07.2017.

technological advance, the evolution of transport and communications routes, etc.), peace is very difficult to be achieve, and the conflict even increased overall in the last decade. This can be observed very clearly if one analyses the data displayed in Figure no. 1.

In this context, where conflict persists and intensifies, theoretical models that can explain, at least partially, how the amplification of tensions is produced (in this case, those concerning the relation between state actors/international actors) are needed. They can provide better knowledge for understanding the current reality, especially in terms of amplification, but also of attenuating regional and international tensions.

Thus, the security dilemma is a concept associated with the framework of analysis the tense relations, such as NATO-Russia relation, the one between the international community (most of all the US) and North Korea, the ones between geopolitical actors which are involved in Syria and so on.

2. The usefulness of the topical security dilemma[2]

We start from the premise that the security dilemma has emerged from the practical need to understand the dynamics of the security environment. Its positive valence is given by the knowledge that this model offers in order to reveal how tensions can emerge, from the weakest states of them, to the most intense stages of conflicts[3].

The security dilemma proposes a spiral pattern of how the insecurity of a system gradually amplifies, based on the interaction between actions and reactions of some actors. For the international reality, security dilemma could provide at least a sequential or partial explanation of the causes and the way in which a state of tension at a regional/global level, at a given time, has been reached.

As in the case of other concepts related to the sphere of international relations, geopolitics and security studies, for the security dilemma there is no academic consensus regarding its constitutive elements and algorithm, as there is no universally accepted definition of it. This term emerged in the ’50s, its “parents” being John Hertz (1950), who, in fact, gave it the name of “security dilemma”, Herbert Butterfield (1951) and Robert Jervis (1970s) - even if Jervis develops ideas in this respect two decades after the first two, we can still consider him as one of the pioneers of the security dilemma, because he associates the notion with a spiral model and also has the merit of incorporating the concept into the theory of international relations.

Over time and till the present days, the security dilemma has been approached from several perspectives, among which we can mention:

- *The offensive realist view*: in an anarchic international system, the fear generated by the intentions of the rival states can distance even two security seeking states from cooperation[4];
- *The defensive realist view* questions the strength of the link between anarchy, uncertainty and cooperation: two security seeking states should not find it difficult to cooperate if they are recognized as being part of this category of states; uncertainty is not enough for offensive realists to formulate pessimistic predictions, even if uncertainty about a state’s motivation can indeed complicate matters[5];
- *Bayesian realism view*: while previous approaches take into consideration two security seeking states, this perspective brings into attention other variables, such as states with different preferences regarding the revision of the status quo and the level of trust between states; there are two distinct categories of countries − trustworthy and untrustworthy.[6]

[2] The present research is based on a previous study, disseminated through a communication presented at the *International Conference* “*Strategic Security Environment: Challenges and Trends*”, organised on 18 May 2017 by the Center for Strategic Defense and Security Studies of the Military Academy of the Armed Forces “Alexandru cel Bun” Chişinău, Republic of Moldova, in process of publication.

[3] See the five levels of conflict structurated by Heidelberg Institute for International Conflict (HIIK), in *Conflict Barometer*.

[4] Avidit Acharya, Kristopher W. Ramsay, “The Calculus of the Security Dilemma”, *Quarterly Journal of Political Science*, Vol. 8, no. 2, pp 183-203, available online at http://stanford.edu/~avidit/security.pdf, accessed on 22.05.2017.

[5] *Ibidem.*

[6] *Ibidem.*

Table no. 1: The algorithm and the main elements of the security dilemma. Progressive perspective

AUTHOR	YEAR*	SECURITY DILEMMA'S ELEMENTS AND ALGORITHM	INNOVATION
John Herz	1950	1. Anarchic system 2. Uncertainty and fear of an actor's intentions 3. Power accumulation in response to fear 4. The power competition cycle can increase the insecurity of the system 5. The security dilemma can lead to war, but it is not the cause of all wars 6. The security dilemma has a self-feeding dynamic, this resulting in a vicious circle	1. Realism beliefs 2.Anarchic system 3.Mistrust among actors SECURITY DILEMMA
Herbert Butterfield	1951	1. Fear 2. Uncertainty about an actor's intentions 3. Unintentional 4. Tragic results 5. Amplified by psychological factors 6. It is the fundamental cause of wars	Unintentional nature
Robert Jervis	1976-1978	1. In an anarchic system, states with compatible objectives can end up in competition, or even in war 2. Two variables give the nature and magnitude of the dilemma: the offensive-defensive differentiation and the offensive-defensive balance	Incorporating the security dilemma into the theory of international relations The term: "spiral model"
Charles L. Glaser	1997	Two key variables: 1. Motivations can go beyond the security seeking need: the greed of an actor 2. Unit-level knowledge of the opponent about the motivations of a country	The concept of "greedy state"
Andrew Kydd	1997-2005	1.Trust issues are at the core of the security dilemma; the level of trust can determine whether, in an anarchic system, cooperation is possible or not. 2. Trust interacts with two variables: relative power and cost of conflict. Depending on their interaction, the degree of cooperation may increase or decrease 3. Uncertainty about the information held by the actors and their preferences 4. The use of Bayesian game theory for analysing the issue of trust / mistrust. Four types of actors are varying according two axes (Axis 1: aggression/greed, Axis 2: the degree of fear) and two rounds of decisions (attack / defence).	The first known approach to the issue of incomplete information in the security dilemma

AUTHOR	YEAR*	SECURITY DILEMMA'S ELEMENTS AND ALGORITHM	INNOVATION
Andrew Kydd	1997-2005	5. Trustworthy states are often able to separate themselves from those unworthy ones. 6. Greedy states are more likely to consolidate their power for expansion (regardless of the nature of their adversary), while security seeking states will opt for consolidation only if they consider their opponent as a greedy one. 7. The spiral of arming can be avoided by security seeking states through refraining from the accumulation of weapons. Greedy states are prone to war, especially if the cost of the war or of the arms race is a lower one.	The first known approach to the issue of incomplete information in the security dilemma
Shiping Tang	2009	1. Starting point: the anarchy of international politics 2. Uncertainty about the actors' intentions 3. Unintentional nature 4. Uncertainty and fear lead to the accumulation of power, which invariably contains offensive components 5. Spiral pattern of worsening relations; arms race 6. "More power, but less security" 7. Vicious circle: serious outcomes can emerge (war) 8. The severity of the dilemma can be amplified by material and psychological factors.	1. Anarchy 2. Unintentional nature: lack of malign intentions 3. Power accumulation SECURITY DILEMMA
Avid Acharya, Kristopher W. Ramsay	2013	1. The issue of trust lies at the heart of the security dilemma (especially the uncertainty about strategic fundamentals: the military technology of the actors, the relative benefits of a military offensive, the incentives for mutual co-operation); the common values environment. 2. The validity of the offensive realism logic: even when states know they are in the category of security seeking ones, trust can be at such a low level that cooperation can become impossible. 3. The security dilemma is not necessarily ameliorated by pre-action discussions (which falls under the diplomacy area).	A formal model showing the low probability of cooperation in certain situations; the role of diplomacy: in many cases, pre-action discussions do not necessarily lead to an improvement in terms of cooperation.

Sources:

Shiping Tang, “The Security Dilemma: A Conceptual Analysis”, *Security Studies*, 18:587–623, Taylor & Francis Group, LLC, 2009, p. 587, available online at https://www.researchgate.net/publication/242166630_The_Security_ Dilemma_A_Conceptual_Analysis, accessed on 02.03.2017.

Charles L. Glaser, “The Security Dilemma Revisited”, *World Politics*, Vol. 50, No. 1, Fiftieth Anniversary Special Issue (Oct., 1997), pp. 171-201, Cambridge University Press, available online at http://www.jstor.org/stable/25054031, accessed on 12.04.2017.

John H. Herz, “Idealist Internationalism and the Security Dilemma”, *World Politics*, Vol. 2, No. 2 (Jan., 1950), pp. 157-180, 1950, p. 157, available online at https://www.jstor.org/stable/2009187, accessed on 02.03.2017.

Evan Braden Montgomery, “Breaking Out of the Security Dilemma - Realism, Reassurance, and the Problem of Uncertainty”, *International Security*, Vol. 31, No. 2 (Fall 2006), pp. 151–185, available online at https://www.jstor.org/stable/4137519, accessed on 19.04.2017.

Avidit Acharya, Kristopher W. Ramsay, “The Calculus of the Security Dilemma”, *Quarterly Journal of Political Science*, Vol. 8, 2013, available online at http://stanford.edu/~avidit/security.pdf, accessed on 15.08.2017.

Andrew Kydd, “Game Theory and the Spiral Model”, *World Policies*, vol. 49, nr. 2, April 997, pp. 371-400.

Andrew Kydd, “Trust and Mistrust in International Relations”, Princeton, New Jersey, Princeton University Press, 2005.

A. N.: Some of the information can be seen, in a different form, also in Cătălina Todor, “Dilema securităţii în actualitate. Spirala tensiunilor NATO-Rusia”, study presented within the *International Conference* “*Strategic Security Environment: Challenges and Trends*”, organised by The Center for Strategic Defense and Security Studies of the Military Academy of the Armed Forces “Alexandru cel Bun” Chişinău, Republic of Moldova, in process of publication.

*A. N.: The year of theoretical developments.

Some of the most important conceptual approaches of the security dilemma are structured in Table no. 1, which shows the continuity of the pursuits in this field and the topicality of the notion.

Broadly speaking, although some variables may differ depending on the perspective and evolution of the concept[7], the security dilemma logic starts from an anarchic international system[8] in which the tensions between actors can gradually increase to the worst level (represented by war), in a spiral pattern of power accumulation. Accumulation of power (due to the actors that want to ensure their own security) can lead to insecurity of the system.

Of course, the accumulation of power (both “soft” and “hard” power) may be motivated either by fear and uncertainty about an actor’s intentions, or by expansionist nationalism geopolitical thinking (from this category one can mention imperialisms, pan-ideas). These would be the two extremes that describe two different typologies of states: security seeking ones and greedy states (categories highlighted by C.L. Glaser since the 1990s). However, we consider that, besides these two typologies, there can also exist another particular category of states, the one of mixed motivated states. From this perspective, one state can have its actions motivated by both of the above mentioned

[7] This concept (security dilemma) evolved over time, as it is often the case of the notions specific to the area of international relations, geopolitics and security studies. On the other hand, the evolution of some concepts like this is also dictated by complex societal developments at global level.

[8] It is defined by the absence of a final political/governance unit to provide international convergence, to which the multitude of states and groups/blocks/international organizations are subordinated to.

factors, this leading accumulation of power. For example, a so-called greedy state can be motivated to accumulate power both through an expansionist geopolitical view, but also through envisioning a threat as possible and real. This can arise from the loss of some traditional spheres of influence, considered to be vital for its security (an example in this regard could be Russia). Hence, from this emerges the difficulty to put in a certain category the actions of a state: if they are intentional or unintentional, aggressive/offensive, or motivated by fear/defensive ones. Thus, if we are discussing about a mixed-motivated state (placed between defining its own security and an existence of a history that presents examples of an expansive geopolitical view and practice), then its actions can be a blend between intention and unintentionally, between defensive and offensive. Therefore, it is very difficult to make a clear delimitation of situations and to conclude that certain developments do not fall into the security dilemma pattern (like there is the case of tense situations caused by the power accumulation of some greedy states).

The hypothesis of incomplete information (to which Andrew Kydd draws attention) accentuates this difficulty. Also, due to the possible existence of states where motivation is a mix of fear and great powers geopolitical thinking, often marked by expansionism (although not necessarily in the purely territorial sense, but expansionism manifested at the level of sphere of influence), we consider that most of the regional and global tensions/conflicts are within the logic of the security dilemma.

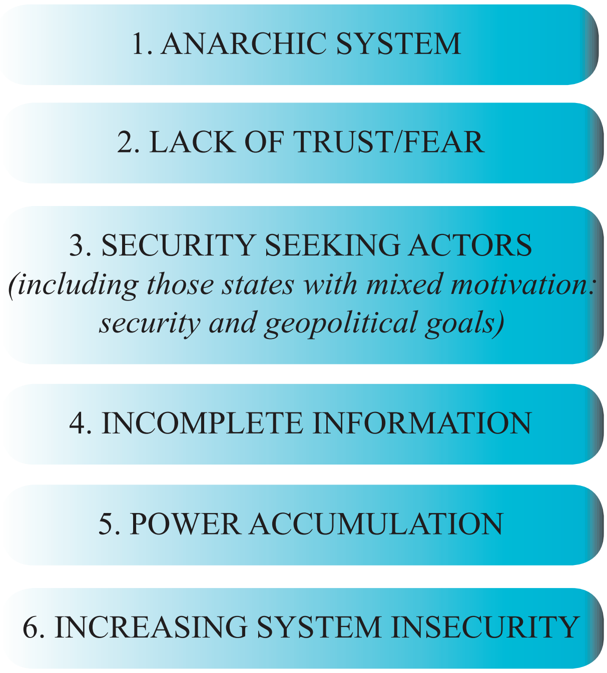
Through this exposing, we pursued two objectives:

- Emphasizing that this concept has topicality and it is evolving in time, having different variables. Two distinct motives are at the core of this: firstly, this concept has been designed to serve understanding how some situations that threaten system's security can be reached, and secondly, its evolution is in relation to the security environment which it tries to explain. And one must take into account that this environment is in a continuous dynamic and transformation.
- Pointing out what are the most important constituent elements of a security dilemma relation pattern.

3. Theoretical framework for validating a relation between actors as a security dilemma pattern

We can draw from previous chapter's analysis the six most important elements of the security dilemma in topicality. Thus, when we identify that a relation between certain actors meets all this six conditions (elements) from Figure no. 2, we can assert that particular dynamic is following the logic of the security dilemma pattern.

From that point on, the spiral pattern can be used as theoretical framework for analysing the developments of that relation. This can evolve into three types of directions: improvement of the situation in terms of accumulation of power and insecurity (decreasing tensions in the relations), increasing the accumulation of power and the insecurity of the system (increasing tensions in the relations), and maintaining the degree of power and security without significant fluctuations (freezing the spiral development of a relation).



1. ANARCHIC SYSTEM

2. LACK OF TRUST/FEAR

3. SECURITY SEEKING ACTORS
(including those states with mixed motivation: security and geopolitical goals)

4. INCOMPLETE INFORMATION

5. POWER ACCUMULATION

6. INCREASING SYSTEM INSECURITY

Figure no. 2: The constituent elements of the topical pattern of security dilemma

Analysing each of the six elements, within a specific relation between certain actors, can provide information on the direction (one from the three previously mentioned) in which the interaction between the parties may lead.

In the following, are presented three additions that could bring more clarity related to some of these six constituents elements of the security dilemma. We are going to bring more information regarding the components three, five and six:

- *Component no. 3*: actors must be in the category of those who are security seeking, for which there is and prevail the unintended nature of actions, even if some of them may lead to an increase in tension. We also include here those actors motivated by a mix of security seeking reasons and of preserving some geopolitical goals specific to the expansionist logic in the spheres of influence; for some actors, threatening such goals may transform into a threat perception for their own security.
- *Component no. 5*: the power accumulation takes into consideration the complex meaning of the concept of power. It must be seen as a mix of the hard component – tangible component/quantitative indicators such as military strength, economic capacity, demographic capacity, natural resources, territory, infrastructure, technology - and the soft component - intangible component/qualitative indicators - national cohesion, representation at regional/world level, political leaders, the ability to organise and effectively govern the society, the level of culture and civilization, the power of tradition, the determination of population in achieving objectives, education, professional training, information component, propaganda, etc. [9].
- *Component no. 6*: The increase of system's insecurity occurs as a result of accumulating power from the behaviour of actors which aim to ensure their own security. This leads to a vicious circle, to a power accumulation spiral because the other actors involved in the equation feel a potential threat. As a result, those other actors may decide also to enhance their power in order to ensure their own security. This type of dynamics can result in an arms race, a notion that, moreover, was and is been associated with this concept of security dilemma. On the other hand, given the fact that power does not consist only of its hard component, besides this armament race, a race of strengthening the intangible component of power (the "soft" one) it is possible to occur. Here one can include also the consolidation of those skills and capabilities that support the ability to manage and control one's actor security, but also the ability to influence regional or even international security. This often can contribute to an actor's empowerment in imposing or playing a major geopolitical role in different spaces (from traditional ones such as: land, sea, air, to the emerging ones, such as cyberspace and the sphere of representation in a population's consciousness). Particularly in the present days, the soft component of power gains new valences, the information society providing a new space in which both convergent and divergent positions can be manifested by actors. This new space is the cyber space (fake news, propaganda, etc.). Power accumulation, in both its components, by actors involved in a relation following a spiral pattern can lead to a deterioration of the relation and to a potential degradation of the regional/global security environment.

If a situation/relation meets all six components, we can classify it as a security dilemma issue that follows the spiral pattern logic. The knowledge generated by this algorithm can contribute to a non-exhaustive understanding of how the amplification/attenuation of tension at regional and international level can happen.

[9] Information previously used in other researches, for example in: Cătălina Todor, "Dilema securității în actualitate. Spirala tensiunilor NATO-Rusia", study presented at the *International Conference "Strategic Security Environment: Challenges and Trends"*, organised by The Center for Strategic Defense and Security Studies of the Military Academy of the Armed Forces "Alexandru cel Bun", Chişinău, Republic of Moldova, in process of publication and Cătălina Todor, "From Classical Geopolitics to Contemporary Geopolitics. Statutory Elements of a Strong Grounded Science in Reality and Actuality", *Geopolitical Perspectives and Development EUBSR 2013 International Conference Volume*, 2013, Italian Academic Publishing, p. 168.

That is why we believe that this concept can be methodologically used to analyse the dynamics of a relation between actors involved in the international security environment.

Conclusions

As it can be observed from the first part of this article, the current security environment is not a more stable one, despite increased interdependencies and interconnections at international level. Therefore, any concept or methodological framework that supports the understanding of security dynamics, even partially, has an immediate utility. This is also the case with security dilemma.

The second part of the research shows that the spiral pattern offered by the security dilemma has evolved over time. Authors who studied it added new variables or drew attention to possible arguments that might dismantle it (e.g. Glaser's developments on the existence of greedy states that annul the security dilemma logic). However, the most relevant approaches on the subject show that some elements of the security dilemma remain constant: the anarchic system, lack of trust, the accumulation of power and increase in the system's insecurity.

Studying the literature, we came to the conclusion that a topical model for the security dilemma could be constituted by the existence of six conditions: 1. an anarchic system, 2. the lack of trust, 3. the existence of security seeking actors (including those with mixed motivation), 4. incomplete information, 5. power accumulation, 6. increased system's insecurity.

We consider that if all these characteristics within a relation between two or more actors of the international security environment are met, then the relations fall within the spiral pattern offered by the security dilemma.

We conclude by asserting that the practical valence of this research is the possibility of using the logic of the six characteristics existence in case studies. Besides, as a continuation of this research, we propose to offer an example in a future article by studying the relation between NATO and Russia through these six elements in order to demonstrate whether we can discuss about security dilemma in this case or not.

BIBLIOGRAPHY:

1. ***, *Conflict Barometer*; Heidelberg Institute for International Conflict (HIIK), available online at https://www.hiik.de/en/konfliktbarometer/.

2. ACHARYA, Avidit; RAMSAY W. Kristopher, "The Calculus of the Security Dilemma", *Quarterly Journal of Political Science*, Vol. 8, no. 2, pp. 183-203, available online at http://stanford.edu/~avidit/security.pdf.

3. BRADEN MONTGOMERY, Evan, "Breaking Out of the Security Dilemma - Realism, Reassurance, and the Problem of Uncertainty", *International Security*, Vol. 31, no. 2 (Fall 2006), pp. 151–185, available online at https://www.jstor.org/stable/4137519.

4. GLASER, L. Charles, "The Security Dilemma Revisited", *World Politics*, Vol. 50, no. 1, Fiftieth Anniversary Special Issue (Oct., 1997), pp. 171-201, Cambridge University Press, available online at http://www.jstor.org/stable/25054031.

5. HERZ, H. John, "Idealist Internationalism and the Security Dilemma", *World Politics*, Vol. 2, no. 2 (Jan., 1950), pp. 157-180, 1950, available online at https://www.jstor.org/stable/2009187.

6. KYDD, Andrew, "Game Theorz and the Spiral Model", *World Policies,* vol. 49, no. 2, April 1997, pp. 371-400.

7. KYDD, Andrew, "Trust and Mistrust in International Relations", Princeton, New Jersey, Princeton University Press, 2005.

8. TANG, Shiping, "The Security Dilemma: A Conceptual Analysis", *Security Studies*, 18:587–623, Taylor & Francis Group, LLC, 2009, available online at https://www.researchgate.net/publication/242166630_The_Security_Dilemma_A_Conceptual_Analysis.

9. TODOR, Cătălina, "Dilema securității în actualitate. Spirala tensiunilor NATO-Rusia",

study presented at the *International Conference* "*Strategic Security Environment: Challenges and Trends*", organised by The Center for Strategic Defense and Security Studies of the Military Academy of the Armed Forces "Alexandru cel Bun", Chişinău, Republic of Moldova.

10. TODOR, Cătălina, "From Classical Geopolitics to Contemporary Geopolitics. Statutory Elements of a Strong Grounded Science in Reality and Actuality", *Geopolitical Perspectives and Development EUBSR 2013 International Conference Volume*, Italian Academic Publishing, 2013.

INSTITUTIONAL RESILIENCE GROWTH TO COUNTER NATIONAL SECURITY THREATS

*Ştefan SĂVULESCU**
*Mihaela ŢONE***

Due to the dynamics of the global security, corroborated with the increased globalization effects states, military alliances and other cooperation organizations are facing huge challenges for maintaining the level of security reached in the last decade. These developments caused NATO and EU Member States to adopt conceptual and operational level measures, of a nature to change the paradigm in which were designed part of the mechanisms for ensuring own citizens' protection and defending fundamental human rights. If NATO established as a priority to take measures at state level in order to develop resilience against threats, in accordance with the regulations of Article 3 of the Alliance Treaty, EU took into serious debate the option of constituting a European military force. On the other hand, at the Members State level, there was developed an effective cooperation amongst military structures and law enforcement ones. This tendency also manifested itself at our country's level. Romania developed institutional mechanisms needed for managing national security threats, in accordance with NATO and EU requirements regarding resilience and the maintenance of a higher safety level for its own citizens, similar to European states' level.

Keywords: *resilience, inter-institutional cooperation, migration, solidarity, national and European mechanisms, European Union, NATO, hybrid threats.*

1. The Evolution of the security and institutional adaptability (at allied, European and national level)

The evolution of the security registered at the end of the 20th century met an unprecedented dynamic, which imposed rethinking the paradigm of taking action, not only at state and military alliances level, but also in regard with international cooperation organizations.

The fall of the Iron Curtain during the 90's, the terrorist attacks from 9/11/2001 on the World Trade Centre Twin Towers from New York City, the evolution of the Middle East security situation, starting with the year 2010, along with the outburst of "Arab Spring" and the boosting of the migrational phenomenon represent main landmarks of the past three decades. Their development, concomitantly with the dynamics of some state actors (such as the Russian Federation) aiming to enlarge or strengthen the area of influence contesting state

Police Chief Commissioner Ştefan SĂVULESCU is the Chief of Operations Directorate within the General Directorate for Operational Management of the Ministry of Internal Affairs, Bucharest, Romania. E-mail: stefan.savulescu@mai.gov.ro

*****Police Commissioner Mihaela ŢONE is a Specialist for the Inter-institutional Cooperation Office within the General Directorate for Operational Management of the Ministry of Internal Affairs, Bucharest, Romania. E-mail: mihaela.tone@mai.gov.ro***

border limitation and maintaining the interest of the population from different regions in order to obtain autonomy based on ethnical criteria and the expansion of terrorist attacks have imposed the adaptation of the mechanisms designated for managing those types of phenomena.

NATO's extension period, after the fall of the Iron Curtain in the 1990 and the 9/11 terrorist attacks, together with the strengthening of its position in the member countries and in the action areas was followed another period in which NATO is constantly reevaluating and transforming its policies, capabilities and structures, in order to assure that it may continue to address the current and future challenges, for the freedom and security of its members[1].

The alliance adapted its capabilities, taking action for extending its sphere of action, from purely military, to fighting terrorism and crisis situation management. Thus, in addition to reevaluating the operating policies, NATO pursued the supplementation of the budgets allocated to the competent ministries and the growth of states' resilience.

Understood as a corollary of deterrence and reassurance measures in the classical military sphere of comprehensive security strategy, resilience is evaluated on the basis of seven fundamental requirements[2]:

1) assuring continuity of government and critical government services;
2) resilient energy supplies;
3) ability to deal effectively with massive movement of people;
4) assuring food and water resources;
5) ability to deal with mass casualties;
6) resilient communication systems;
7) resilient transportation systems.

The European Union has faced profound changes, gradually turning from a solely economical union, to an organization which takes action in various domains, from politics, to climate change, environmental protection and health, to foreign and security relations or justice and migration.

The security of its own citizens has known a high, unprecedented level, in comparison to many other world regions, as an effect of the security measures adopted by each member state and the international cooperation mechanisms applied, but also as a result of the positive effects of globalization in the technologic, politic or economic fields. However, the recent evolution of the security situations from the European continent proximity and from the interior of the continent, actions of some state/non-state actors or even of some extremist movements' exponents led to changing state borders, to the persistence of the frozen conflicts' manifestation and instilling an insecurity feeling amongst Europeans.

These developments corroborated with the negative deepening globalization effects determined states to identify solutions for interconnecting military and non-military elements, increasing institutional resilience and developing cooperation at all relevant levels, more specifically, military, public order, economic, intelligence, technic, science, education, etc.

The eight terrorist attacks committed in Europe in less than six months in France, Sweden, Russia, Great Britain, Turkey and Germany, between December 2016 - May 2017, initiated within the context of the subsequent applied measures to a higher alert level of law enforcement institutions, prove, on one hand, the adaptability of the actions carried out by the extremist organisations' exponents, and on the other hand, the necessity of adopting complementary measures, in order to maintain the security level, reached at the beginning of this decade.

The actions of institutions bearing direct responsibilities are insufficient without the permanent adaptation of international cooperation mechanisms, the coordinated involvement of resources which each state has at their disposal and the continuing processes conducted for educating their own citizens, in order to address an attitude of supporting law enforcement agents.

[1] Adapted from the Secretary General"s Annual Report 2016, Investing in Security, p. 28, available online at http://www.nato.int/cps/en/natohq/opinions_142149.htm#sg2, accesed on 12 May 2017.

[2] Resilience: a core element of collective defence, available online at http://www.nato.int/docu/Review/2016/Also-in-2016/nato-defence-cyber-resilience/EN/index.htm, accesed on 12 May 2017.

In the search of balanced solutions for managing the present security situation, the concerns at European level have refocused towards complex interconnected and transnational threats and there have been concrete discussions about launching, in the near future, an armed force at European Union level.

Furthermore, at European level, it is assessed, more than ever, that "aspects like human rights, environment degradation, political stability and democracy, social issues, cultural and religious identity or migration should be taken into be consideration"[3].

In the last decade, the main threat the European states had to face was irregular migration, the peak being recorded in 2015, when the immigrants' number that reached Europe exceeded one million[4].

This phenomenon tested not only the solidarity and the cooperation mechanisms at European level, but also national authorities' level of preparedness for managing a crisis situation.

Although regular migration has positive implications on the labour unemployment market, by decreasing unemployment level and gathering specialists in some vital domains, or on the negative European[5] demographics of over 8% until year 2050, in comparison with the estimated growth for U.S.A. and Canada of approximately 31%, in the current context, when the number of illegal migrants increased significantly, the European Union doesn't afford this growth to take place uncontrolled and without being in accordance with the international and national legislative framework applicable in this domain.

In order to manage this phenomenon, the European Union adopted a set of measures, destined especially for increasing the security level of the external borders, relevant being the adoption of Regulation (EU) no. 2016/1624 of the European Parliament and of the Council, dated 14th of September 2016, regarding the Border Police and Coast Guard at European level[6]. On the other hand, Member States reevaluated the legislative framework regarding migration and political asylum and adopted a number of measures at operational level. Also, in support of EU efforts and the states affected by the migratory phenomenon, there took action governmental and nongovernmental organizations (International Organization for Migration, United Nations High Commissary for Refugees, Doctors without Borders, etc.).

According to Regulation no. 1624, the measures adopted at community level targeted the integrated management of borders at national level, and at European Union level, as a fundamental component of a free, secure and just space, on four levels, and measures in third countries (respectively, like those within the frame of common policies regarding visas), measures with neighbouring third countries, control measures at external borders, risk analysis, and measures within the Schengen area and the field of returning people.

Following the impact of FRONTEX's actions at the European Union border, it has been decided to extend the main operations' scope, and also the duration of Triton and Poseidon missions. In January - August 2016 only, the watercrafts coordinated by FRONTEX saved 76,229 human lives in the Mediterranean Sea, 38,750 of which in the vicinity of Italy, and 37,479 in the vicinity of Greece[7].

[3] European Commission, HORIZON 2020, The EU Framework Programme for Research and Innovation, Security, https://ec.europa.eu/programmes/horizon2020/en/area/security, accessed on 12 May 2017.

[4] Risk Analysis for 2016, FRONTEX, p. 5, available online at http://frontex.europa.eu/publications/?p2, accessed on 12 May 2017.

[5] Europe's *Demographic Future. Growing Imbalances*, written by Berlin Institute, 2016, p. 3.

[6] The regulation (UE) 2016/1624 of the European Parliament and Council *dated 14th of September 2016, regarding the Border Police and Coast Guard at European level* and modifying Regulation (EU) no. 2016/399 of the European Parliament and Council and abrogating Regulation (CE) no. 863/2007 of the European Parliament and Council, of Regulation (CE) no. 2007/2004 and Council, and Decision 2005/267/CE, available online at https://publications.europa.eu/ro/publication-detail/-/publication/65db3442-7bcf-11e6-b076-01aa75ed71a1/language-ro, accesed on 12 May 2017.

[7] EU operations in the Mediterranean Sea, available at https://ec.europa.eu>fact-sheets>docs, accesed on 12 May 2017.

At the same time, at European Union level, there have been taken measures regarding the relocation of asylum seekers within EU Member States, the most important ones being the voluntary resettlement of people in difficulty from neighbouring countries, the return of people who fulfil the conditions for asylum, the conclusion of the EU-Turkey Agreement, in order to limit the influx of migrants, on one of the main routes from the Aegean Sea and to facilitate a reception centres network in Greece and Italy (so called hotspots).

The legislative and operational effort carried out at European level has been complemented with measures adopted by the affected member states, which were extremely heterogeneous. Some states, like Romania and Bulgaria have tried to manage the phenomenon by progressively engaging the resources of law enforcement institutions and strengthening the capabilities to manage it, while others introduced border controls, despite the fact they are part of the Schengen Area, involved the Armed Forces in securing the borders or built artificial barriers (e.g. between Hungary, Serbia, Slovenia and Croatia, between Macedonia and Greece, between Bulgaria and Turkey).

In addition to the measures set up for securing the borders, for the states on the maritime border of Europe (Turkey, Greece and Italy) and those on the migrations routes (Serbia, Croatia, Hungary, Austria and Slovenia), supplying the migrants with food, water, shelter and medical services represented an enormous challenge.

Despite de huge efforts made at European Union and Member States level to secure the borders and respect the fundamental principles of human rights by protecting people in difficulty, at both Community and some Member State level, there were taken into discussion and analysis the action mechanisms for assuring an integrated and coherent management of crisis situations.

Although, at European level, some states were not severely affected by the migration phenomenon or were not in a position to manage security situations crisis, such as Romania, the dynamic of the security environment and recent developments in NATO's eastern flank and the EU, as well as the grim forecasts of a possible de-escalation of conflicts within migrants' countries of origin, require that preventive measures to be taken at all levels to ensure sufficient capabilities and calibrated response mechanisms.

2. Present background and projections concerning cooperation within the operational area, on components in the responsibility of the Ministry of Internal Affairs

If until a decade ago, the majority of the Armed Forces was trained only for purely military actions deployed in hostile environments, familiar to relating doctrines, and the law enforcement bodies were prepared to deal with the security challenges from some individuals, whether organized or not in criminal groups, or to manage emergency situations, recent developments of the security environment have proven that a clear operating line can no longer be ascertained between the two essential security branches, from the responsibility of the Ministry of National Defence and Ministry of the Internal Affairs.

The trend in this domain is represented by the recalibration of national and NATO military structures' capabilities to be able to cope with a broader spectrum of action and ensuring the interoperability within other security responsible institutions.

The measures adopted by the Armed Forces are doubled by those launched, on NATO's initiative, by the national institutions, in order to raise the resilience level of states, sense into which had been defined the seven action areas before mentioned.

In the case of Romania, the cooperation between the Ministry of National Defence and Ministry of Internal Affairs has met an accelerated boost in the last years, not only conceptually, but also operationally. Although successfully concluded, the real or practice drills undertaken jointly have brought into attention the need of interoperability level growth and thorough understanding of the challenges that every structure within these institution faces.

The Ministry of Internal Affairs, in addition to borrowing best practices used at NATO level and, implicitly, at the level of the Ministry of National Defence, implicitly, developed its structural component of missions and operations planning, establishing, within its headquarters, the Operations Directorate. Through this measure has been managed the development of institutional capacity for complex mission planning and for creating the necessary premises in order to assure increased interoperability among the other National Defence System, Public Order and National Security institutions.

On the other hand, analysing the law enforcement institutions' responsibilities for ensuring a special situation or a crisis situation management, including during exceptional states - of emergency, siege, deploy and war - it follows that, although the main responsibility is transferred between the institutions in charge, they stay solidary to the national managing effort.

Thus, we appreciate that neither Member States, nor NATO and EU, respectively, afford to use all capabilities available to them in order to manage a crisis state, irrespective of its nature - military or nonmilitary.

3. General aspects and implications regarding inter-institutional cooperation concerning national security

At present, one does not have a coherent image of how the security environment will look like, in the future, although one thing is certain: the magnitude, purpose and complexity of the security threats have reached a point at which no sector - be it governmental, civil society, economic, social, academic - can manage by itself the occurring transformations[8].

However, even if at European Union level there aren't any more armed conflicts, present threats are circumscribed both to the military and the civilian field, gaining more and more a hybrid aspect. Hence, recent events that took place within the European area (annexation of Crimea by the Russian Federation, the influx of migrants originating in the Middle East and Northern African states, terrorist attacks, as well as cyber-attacks), confirm the hybrid nature of threats against European and national security.

In this context, in order to deal with all these challenges, it is required to establish alliances between different actors and for these to achieve an inter-institutional cooperation, context in which the cooperation and coordination at ministry level is a must, in order to achieve output that cannot be obtained individually.

Consequently, according to the National Defence Strategy (2015)[9], the objectives and operation lines that concern national security aim to strengthen not only military capability, but also civilian ones, to standards which enable prevention, deterrence and defence against any aggressive actions towards our country, including hybrid ones.

Even though inter-institutional cooperation seems to be the right answer in order to face current threats, it should be pointed out that efficient cooperation implies expenses, especially regarding time. Signing cooperation agreements/ protocols fails to provide necessary premises for an efficient answer to security threats, but operationalization and practical testing of these protocols, as early as peacetime, are prerequisites that can improve the institutional response at national level.

From the practical experience in the field of national security, I concluded that, in order to be efficient, inter-institutional cooperation requires complying with some principles:

- shared values;
- understanding mutual expectations, capabilities and limitations;
- mutual commitment;
- specific platforms for exchanging Intel;
- leadership;
- planning during peacetime;

[8] National security, https://en.m.wikipedia.org/wiki/National_security, accesed on 10 May 2017.

[9] National Defense Strategy for the period 2015-2019 - A strong Romania within Europe and the world, Bucharest, 2015, available at http://old.presidency.ro/static/National%20%20Defense%20Strategy%202015%20-%202019.pdf, accesed on 10 May 2017.

- joint drills.

Furthermore, in particular, the inter-institutional cooperation between the Ministry of Internal Affairs and the Ministry of National Defence may involve supporting civilian authorities with military operations, in certain situations like disasters, flux of migrants, paramilitary actions of non-state players, etc. In this context it is important that each involved party to understand the delimitation of their own duties, in relation to the subject area, as well as their respective responsibilities, by a continuous process of planning and drill driving, given that in a crisis situation, the level of trust cannot be immediately increased.

An extremely important role in promoting and assuring inter-institutional cooperation regarding national security is held by the Supreme Council of National Defence (SCND), autonomous administrative authority which uniformly coordinates the activities that concern our nation's defence and national security, in accordance with the provisions of Romania's Constitution.

For the first time, at national level, the concept of an inter-institutional cooperation and coordination body in the area of national security, was envisaged by the Constitution written in 1923, which stipulated in article 122 that a Supreme Council of National Defence will be established to provide on a permanent basis, the necessary measures for coordinating national defence[10].

At present, the responsibilities and the activity of the Supreme Council of National Defence are governed by the regulations of Law no. 415/2002, regarding the organisation and operation of the Supreme Council of National Defence, and both the Ministry of Internal Affairs and the Ministry of National Defence, together with other institutions, are components of this collaborative format.

Each institution which is member of the Supreme Council of National Defence has its own way of managing the decisions/documents, as well as the activity in this area. Representatives of the institutions that are members of the Supreme Council of National Defence attend its meetings, in order to ensure national security; nevertheless, it is still required to develop an inter-institutional cooperation format, at different levels and depending on specific topics, due to the fact that the Supreme Council of National Defence doesn't have a crisis unit role.

However, the Supreme Council of National Defence, through it's carried out duties, has a well determined role, especially regarding the analysis and approving of strategy papers which address national security, of measures regarding the rejection of armed aggressions aimed against Romania, but also regarding the coordination of some activities subsequent to our country's integration in the European and Euro-Atlantic security structures. Consequently, in accordance with the provisions of Law no. 415/2002, the Supreme Council of National Defence "coordinates the activity of integration in the European and Euro-Atlantic security structures, monitors the armed forces adaptation process under the regulations of NATO and makes recommendations in accordance with the Alliance standards"[11], therefore, the role of the Supreme Council of National Defence is that of a decision-making tool regarding the national security policy.

Moreover, security climate planning, at national level, is a shared responsibility, of all affiliated institutions, not only of the Supreme Council of National Defence or the two aforementioned ministries, and an important part of this process includes the civil society. The development of the security culture is a necessity, not only at institutional level, but also at private-sector level and among citizens.

Taking into account the given considerations, we can conclude that, regarding national security,

[10] Author's translation from Romania's Constitution 1923 apud Sever Voinescu, Constantin Dudu Ionescu, Consiliul Suprem de Apărare a Țării, principal instrument de decizie în politica de securitate a României (Supreme Council of National Defence, the main decision-makink tool in the Romanian security policy), Institute for Public Policy, Bucharest, 2005.

[11] Author's translation from Law no. 415/2002 regarding the organisation and operation of the Supreme Council of National Defence, as subsequently amended and supplemented.

inter-institutional cooperation requires integrated actions, robust capabilities, including ISR (Intelligence, Surveillance, Reconnaissance), as well as ample and complex operations, for a contextualized approach of the present security threats.

The implementation of the seven basic requirements of resilience – example of inter-institutional cooperation

As previously mentioned, in order to grow national resilience, the North Atlantic Council has established seven basic requirements, as early as February 2016, and, subsequently, at Alliance level, have been developed guides and evaluation criteria to assist each Member State during the evaluation and planning/instruction process, in order to manage crisis situations[12].

Considering the fact that the term resilience means the capacity of a system to deal with potential or current crisis situations that can occur and continue to develop, we can appreciate that the evolution of national resilience, in order to deal with any type of threats, is a continuous process with no ending date.

Taking into consideration the importance, at Alliance level, given to developing national resilience by each member state, during July 2016 Warsaw NATO Summit, the head of states and governments assumed, as a priority, the implementation of the seven basic requirements.

Romania joins this endeavour, at national level, the institution responsible for coordinating the implementation of the resilience concept in regard to civilian emergencies being the Ministry of Internal Affairs. Therefore, in this concept implementation process, several institutions were invited to make a contribution: the Presidential Administration, the General Secretariat of the Government, the Ministry of Foreign Affairs, the Ministry of National Defence, the Ministry of Internal Affairs, the Ministry of Agriculture and Rural Development, the Ministry of Health, the Ministry of Energy and the Ministry of Transportation, thus succeeding to develop a national inter-institutional cooperation mechanism.

The line ministries assumed the responsibility to develop specific mechanisms within the competence area, in order to grow resilience in communications, transportation and water and food resources sectors. As concerns the establishing of national mechanisms for managing uncontrolled population displacement and multiple victims, the responsibility has been assumed by the Ministry of Internal Affairs.

By implementing the resilience, at national level, it is considered, on one hand, the developing of the institutional capacity in order to handle any threats, including hybrid ones, but also the developing of the national capabilities interoperability with those of NATO, whereby, in case of necessity, the host nation support can be assured for allied forces.

Furthermore, bearing in mind that 90% from the resources and logistics necessary to NATO forces derive from private companies or are provided through contracts with private-sector operators, in this process have been involved, subsequently, private operators, either from transportation, communications, or food sector, endeavouring the achievement of a common standard of understanding military requirements, at a civil/private sector level.

Additionally, in the present context, in which a clear delimitation of peace and war concepts does not exist anymore, by the appearance of hybrid threats, the singular actions of state forces became insufficient, requiring concerted actions, together with civil-sector players (i.e. from communications sector).

Furthermore, the hybrid threats require not only cooperation between the military and the civil sectors[13], but also collaboration between organizations, like the collaboration between

[12] Allies move forward on enhancing NATO's resilience, available at www.nato.int/cps/en/natohq/news_135288.htm?selectedLocale=en , accesed on 12 May 2017.

[13] Cătălin Alexandru, Patrick Turner (NATO): Romania, one of the powerfull allies of NATO regarding the measures for increasing the resilience, https://www.agerpres.ro/politica/2017/03/28/patrick-turner-nato-romania-unul-din-cei-mai-puternici-aliati-nato-in-masurile-de-crestere-a-rezilientei-12-54-13, 28.03.2017, accesed on 29 March 2017.

NATO and EU, especially in regard with resilience growth and hybrid threats counteracting, as well as other resources, including legislature, of EU.

At national level, in the matter of hybrid threats, in the professional practice we identified the main institutional responsibilities, assessed from the correlation of the types of hybrid threats with the necessary measures to counteract them, considering the following aspects:

- permanent acknowledging of the operative situation, matching the sphere of competence;
- preventing hybrid type actions, through increasing the measures of physical protection of the objectives found in accountability, as well as securing information and communication networks;
- leading and implementing actions for counteracting, in the event of occurring on the national territory;
- increasing the level of interoperability and Intel exchange between the structures within the National Defence System;
- completing schedule, training and inter-institutional cooperation documents, for the purpose of increasing action capacity, in an integrated manner, of institutions within the National Defence System;
- taking part in inter-institutional forms of training, within the area, through exercise planning, organising and deployment.

Conclusions

The new challenges to states' security, like irregular migration, repeated terrorists attacks, but also the negative effects of globalisation, require measures to change the paradigm in which were conceived part of the mechanisms to ensure the protection of their own citizens and the defence of fundamental human rights.

So, the states have been determined to identify solutions for the interconnection of military and non-military elements, to increase institutional resilience and to develop cooperation on all relevant levels, namely military, public order, economic, information, technology, science, education, etc.

Both on allied level and on national level, the defence/allied forces' actions require continuous adaptation towards actual vulnerabilities and threats which arise including from non-state players and in terms of real actions or exercises run in common by the Ministry of National Defence and the Ministry of Internal Affairs, these have brought attention to the need to raise the level of interoperability and of a thorough understanding of the challenges faced by each structure within these institutions.

Therefore, national resilience growth towards any type of threats, including hybrid ones, is a central pillar of defence, contributing to reducing security risks and maintaining state cohesion, independence and national security.

BIBLIOGRAPHY:

1. Agerpres News Agency, https://www.agerpres.ro/politica/2017/03/28/patrick-turner-nato-romanaia-unul-dintre-cei-mai-puternici-aliati-nato-in-masurile-de-crestere-a-rezilientei-12-54-13.

2. Reuters News Agency, www.reuters.com.

3. The European Union Agency for Fundamental Rights, *Fundamental rights of migrants in an irregular situation in the European Union*, 2011, http://fra.europa.eu/en/publication/2012/fundamental-rights-migrants-irregular-situation-european-union.

4. European Union Agency for Fundamental Rights, *European Law Handbook regarding political asylum, borders and immigration*, 2014, http://fra.europa.eu/en/publication/2013/handbook-european-law-relating-asylum-borders-and-immigration.

5. Allies move forward on enhancing NATO's resilience, available at www.nato.int/cps/en/natohq/news_135288.htm?selectedLocale=en.

6. ALEXE, Iris; PĂUNESCU, Bogdan (coordinators), *Study on the immigration phenomenon in Romania. The aliens' integration into the Romanian society*, Editor Soros Foundation Romania, 2011.

7. Berlin Institute for Population and Development, *Europe's Demographic Future.*

Growing Imbalances, 2016.

8. BRETTELL, Caroline B., HOLLIFIELD, James F., *Migration theory*, Publisher New York: Routledge, 2015.

9. CASTLES, Stephen; MILLER, MARK J., *The Age of Migration. International Population Movements in the Modern World*, Fourth Edition, revised and updated, Palgrave Macmillan, 2009.

10. Centre for Global Constitutionalism, Communication from the Commission to the European Parliament and the Council on Guidance for Application of Directive 2003/86/EC on the Right to Family Reunification, 2014.

11. Romanian Constitution, republished, 2003. Department of Economic and Social Affairs, United Nation Organisation, *International Migration Report 2015*, 2016.

12. EU operations in the Mediterranean Sea, available at https://ec.europa.eu>factsheets>docs.

13. United Nations Population Fund and the International Organisation for Migration, *International Migration and Development: Contributions and Recommendations of the International System*, 2013, http://publications.iom.int/system/files/pdf/ceb_gmg_web.pdf.

14. Hotărârea Guvernului 1152/2014 privind organizarea, funcționarea și compunerea Centrului Național de Conducere a Acțiunilor de Ordine Publică (Government Decision no. 1152/2014 regarding organizing, functioning and making up of the National Center for Managing Public Order Actions).

15. Hotărârea Guvernului nr. 117/2014 privind organizarea şi funcţionarea Centrului operaţional de comandă al Guvernului, cu modificările şi completările ulterioare (Government Decision no. 117/2014 regarding the organization and functioning of the Government Operations Command Center, as subsequently amended and supplemented).

16. Hotărârea Guvernului nr. 572/2008, privind constituirea Grupului de coordonare a Implementării Strategiei naționale privind migrația, cu modificările și completările ulterioare (Government Decision no. 572/2008, regarding the establishment of the Coordination Group for the Implementation of the National Strategy regarding migration, as subsequently amended and supplemented).

17. Hotărârea Guvernului nr. 780/2015 pentru aprobarea Strategiei naţionale privind imigraţia pentru perioada 2015-2018 şi a Planului de acţiune pe anul 2015 pentru implementarea Strategiei naţionale privind imigraţia pentru perioada 2015-2018 (Government Decision no. 780/2015 for approving the National Strategy regarding Immigration from 2015 to 2018 and the Action Plan of year 2015 for implementing the National Strategy regarding Migration from 2015 to 2018).

18. Hotărârea Guvernului nr. 94/2014 privind organizarea, funcţionarea şi componenţa Comitetului naţional pentru situaţii speciale de urgenţă, cu modificările şi completările ulterioare (Government Decision no. 94/2014 regarding organizing, functioning and composition of the National Committee for Special Emergency Situations, as subsequently amended and supplemented).

19. Hotărârea Guvernului nr. 943/2001 privind înfiinţarea Grupului Interministerial Român pentru Managementul Integrat al Frontierei de Stat, republicată (Government Decision no. 943/2001 regarding the establishment of the Romanian Inter-ministerial Group for Integrated State Border Management, republished).

20. FAUDE, Benjamin, How Is Inter-Institutional Order Possible In Global Governance, aprilie 2016, available at https://lawlog.blog.wzb.eu/2016/04/18/how-is-inter-institutional-order-possible-in-global-governance/.

21. NATO sees resilience as key issue in AWACS replacement, available at http://www.reuters.com/article/us-nato-arms-id-USKBN0L51SE20150201.

22. The Secretary General's Annual Report 2016, Investing in Security, p. 28, available at http://www.nato.int/cps/en/natohq/opinions_142149.htm#sg2.

23. Resilience: a core element of collective defence, available at http://www.nato.int/docu/Review/2016/Also-in-2016/nato-defence-cyber resilience/EN/index.htm.

24. Risk Analysis for 2016, FRONTEX, p. 5, available at http://frontex.europa.eu/publications/?p2.

25. Institutul pentru politici publice Bucureşti, *Consiliul Suprem de Apărare a Țării, principal instrument de decizie în politica de securitate a României* (Institute for public policies, Bucharest, *Supreme Council of National Defence, core decision maker instrument in the security policy of Romania)*, Bucharest 2005.

26. KING, Russell, *Theories and Typologies of Migration: An Overview and a Primer*, Malmö Institute for Studies of Migration, Diversity and Welfare, Malmö University, 2012.

27. Legea apărării naţionale nr. 45/1994, cu modificările şi completările ulterioare (National defence Law no. 45/1994, as subsequently amended and supplemented).

28. Legea nr. 122/2006 privind azilul în România, cu modificările şi completările ulterioare (Law no. 122/2006 regarding political asylum in Romania, as subsequently amended and supplemented).

29. Legea nr. 346/2006 privind organizarea şi funcţionarea Ministerului Apărării Naţionale, cu modificările şi completările ulterioare (Law no. 346/2006 regarding the organisation and operation of the Ministry of Internal Affairs, as subsequently amended and supplemented).

30. Legea nr. 415/2002 privind organizarea şi funcţionarea Consiliului Suprem de Apărare a Ţării, cu modificările şi completările ulterioare (Law no. 415/2002 regarding the organisation and operation of the Supreme Council of National Defence, as subsequently amended and supplemented).

31. Legea nr. 51/1991 privind securitatea naţională a României, republicată (Law no. 51/1991 regarding Romania's national security, republished).

32. Legea nr. 90/2001 privind organizarea şi funcţionarea Guvernului României şi ministerelor, cu modificările şi completările ulterioare (Law no. 90/2001, regarding the organisation and functioning of the Romanian Government and ministries, as subsequently amended and supplemented).

33. Legea planificării apărării nr. 203/2015 (Law on defence planning no. 203/2015).

34. MARENIN, Otwin, *Challenges for Integrated Border Management in the European Union* - Geneva Centre for Democratic Control of Armed Forces - DCAF 2010.

35. MOREHOUSE, Christal; BLOMFIELD, Michael, *Irregular migration in Europe*, Migration Policy Institute, 2011.

36. Ordonanţa de urgenţă a Guvernului nr. 1/1999 privind regimul stării de asediu şi regimul stării de urgenţă, aprobată cu modificări şi completări prin Legea nr. 453/2004 (Governmental Emergency Decree no. 1/1999 regarding the state of siege regime and the state of emergency regime, approved with amendments by Law no. 453/2004).

37. Ordonanţa de urgenţă a Guvernului nr. 194/2002 privind regimul străinilor în România, republicată, cu modificările şi completările ulterioare (Governmental Emergency Decree no. 194/2002 regarding alien act in Romania, reissued, as subsequently amended and supplemented).

38. Ordonanţa de urgenţă a Guvernului nr. 30/2007 privind organizarea şi funcţionarea Ministerului Afacerilor Interne, aprobată cu modificări prin Legea nr. 15/2008, cu modificările şi completările ulterioare (Governmental Emergency Decree no. 30/2007 regarding the organization and operation of the Ministry of Internal Affairs, approved with amendments by Law no. 15/2008, as subsequently amended and supplemented).

39. Ordonanţa de Urgenţă nr. 105/2001 privind frontiera de stat a României, aprobată cu modificări prin Legea nr. 243/2002, cu modificările şi completările ulterioare (Governmental Emergency Decree no. 105/2001 regarding the state border of Romania, approved with amendments by Law no. 243/2002, as subsequently amended and supplemented).

40. International Organization for Migration, *Migration and the United Nations post-2015 development agenda*, 2013.

41. International Organization for Migration, *Migration Initiatives 2016. Migration governance and sustainable development*, 2016.

42. International Organization for Migration, *World Migration Report 2015. Migrants and Cities: New partnerships to Manage Mobility*, 2016.

43. EU Regulations, https://publications.europa.eu.

44. SARCINSCHI, Alexandra, *Migraţie şi securitate (Migration and security)*, "Carol I" National Defence University Publishing House, Bucharest, 2008.

45. SKELDON, Ronald, *Global Migration: Demographic Aspects and Its Relevance for Development, UN Population Division*, Technical Paper no. 2013/6.

46. National Strategy for Defence for the period 2015-2019 - A strong Romania within Europe and the world, Bucharest, 2015.

47. UNHCR, *Global trends forced displacement in 2015*.

48. VOINESCU, Sever and DUDU IONESCU, Constantin, Consiliul Suprem de Apărare a Țării, principal instrument de decizie în politica de securitate a României, Institutul pentru Politici Publice, București, 2005 (Institute for Public Policies, Bucharest, *Supreme Council of National Defence, core decision maker instrument in the security policy of Romania*), Bucharest, 2005.

49. NATO Website, http://www.nato.int/docu/review/2016/Also-in-2016/nato-defence-cyber-resilience/EN/index.htm.

ADVANCED MODEL FOR CONFIGURING HYBRID AGGRESSION

*Dan-Lucian PETRESCU**

Taking into account the complexity of the contemporary security environment and its high level of uncertainty, I believe that the most appropriate approach to integrated efforts to identify and counteract the hybrid threat and resolve the crises it generates is the proactive approach. This must be grounded in a prospective way of thinking, backed by scientific arguments, which can significantly contribute to determining the keystones of the probable or desired dynamics of the current security situation quo-vadis.

In this context, deepening the knowledge of the concept of hybrid threat, that outlines the modern aspect of the war phenomenon, is a major step in the field of Military Science. In this article, I have pursued the design of an advanced, powerful, controllable, efficient and flexible algorithm meant to determine the hybrid aggression configuration in order to help predict future crisis situations on one hand and plan how to prevent or resolve them, on the other.

Keywords: *hybrid threat, hybrid aggression, proactive measures, structural analysis, cross-over impact.*

Introduction

The hybrid threat is extremely complex and its countermeasures must be likewise. The appropriate response to this type of threat must be configured by cleverly and intelligently accomplishing real trans-disciplinary connections between the top fields of Military Science.

It is important to note that a significant effort is currently being made in the international scientific and operational environment to define the hybrid threat and the ways in which it can be implemented, thus becoming aggression. Taking into account the definitions given by the various researchers who invented the concept – James N. Mattis and Frank G. Hoffman – and studied it – Russel W. Glenn, Valery Gherasimov, Andrew Korybko –, the hybrid threat is defined as *a possible action of a state or non-state adversary which uses adaptive and concerted political, military, economic, social or informational means, in combinations of unconventional and conventional methods, in order to achieve the objectives pursued*.

Considering Nathan Freier's *Quad-chart*[1], the dynamic of hybrid threat involves the concerted action of four types of threats – *traditional* (conventional), *irregular* (unconventional), *catastrophic* and *disruptive*[2] – on the target actor's center of gravity, leading to its destruction.

Additionally, an important feature can be inferred from the fact that in the hybrid operational environment, the proportion of actions, from the perspective of typology, displays a strong migration from regular to unconventional,

[1] Nathan P. Freier, "Present at the Counterrevolution: An Essay on the 2005 National Defense Strategy and Its Impact on Policy", *United States Army War College Guide to National Security Issues*, Vol. 2: *National Security Policy and Strategy*, pp. 120-121. Editor J. Boone Bartholomees, Jr., 4th edition, July, 2010.

[2] The disruptive threat may be generated by "disruptive technology" or "disruptive social behavior" (Frank Hoffman).

Lieutenant-colonel Dan-Lucian PETRESCU is Superior Instructor at Defence snd Security Faculty, within "Carol I" National Defence University, Bucharest. E-mail: dan_petrescu1@yahoo.com

especially to asymmetric ones.

In the specific studies, authors prefer to use the term *hybrid threat* instead of *hybrid aggression*. I think the reasons could come from the following two situations. On one hand, it is worth highlighting the proactive character of actions taken to counteract the hybrid aggression by eliminating the threat before it becomes aggression (however, it does not take into account the situation in which a threat may become, itself, an aggression).

On the other hand, there are no regulations or laws whereby a complex of actions could officially be declared aggression of hybrid type.

Table no. 1: Threats that may arise in the operational environment

DOMAIN	THREAT/ AGGRESSION	MEANS	EFFECTS	R	I	IP	OF
POLITICAL	Undermining public confidence in government authorities	Opinion makers, information, time	Decrease /loss of control over domestic and foreign policy	H	4	0.75	P
MILITARY	Insertion of undercover Special Operations Forces (SOF) that would act as local militias	SOF, mercenaries, money	Creating a reason for military intervention or destabilizing internal order	H	4	0.75	M
ECONOMIC	Undermining the external economic relations of the target on its critical areas (e.g. export of resources) through unfair competition or blackmail	Economic resources, influence	Reduce revenues to the state budget, affecting the process of economic development	H	4	0.75	P
SOCIAL	Infiltration of opinion makers to polarize the population in the target state	Specialized staff, information, time	Affecting social cohesion	L	2	0.5	P
INFORMATION	Promoting the inefficiency of the authorities or the incompetence of the political class through opinion-makers (in mass-media or the virtual environment)	Opinion makers, information, circumstances, time	Decrease population support to government authorities and structures	M	3	0.75	P
INFRASTRUCTURE	Destruction of critical infrastructure assets (power plants, permanent crossings, etc.)	FOS, mercenaries, information	Destruction, victims or damage to life of society	H	4	0.75	L
SECURITY	Undermining the authorities in the target state (internal security system, law enforcement system, etc.).	Infiltrated agents, financial resources, information, time	Diminishing the state's ability to secure its own security	H	4	0.75	P

To the extent that in the official documents in the field of public international law, hybrid aggression has not been fully defined, it is deduced that the criteria by which the aggressor can be identified and the aggression can be proved are missing or unclear.

Consequently, the term *threat* is preferred because it provides the formal framework for preventive measures against potential actions, considered aggressions.

Configuring hybrid aggression requires a considerable effort; it has to be accomplished through a complex process, similar to the operational planning (the product is a series of actions in all fields assimilated to military operations) and must be carried out by a least rational, if not super-rational, actor. If the target perceives the aggressor's actions as irrational, it means that the underlying hybrid aggression is well configured and applied. The more irrational the aggression looks, the more it grows in value and amplifies its effects, and the target will be more difficult to generate an adequate response.

Developing the hybrid aggression configuration model

1. The third step is to ***identify the aggressor and the target***. Considering the general case involving the possibility of triggering a hybrid conflict between any of the actors in the operational environment, at this stage we analyze the relationships between actors, for which we recommend the use of the MACTOR[3] method invented by the French analyst Michel Godet. The results obtained offer the possibility of establishing the alliances and conflicts that may arise between the actors and, consequently, the identification of the aggressor and the target. Determined strategies may include making alliances between different actors, resulting in new actors with combined capabilities that may generate hybrid threats in configurations related to their specific components. In order to have the correct image, it is necessary to analyze the composite aggressions and effects pertaining to the resulting parties involved in the conflict. It should also be borne in mind that the structure of the hybrid threat (in quantitative and qualitative terms) depends fundamentally, apart from the generator's capacities, on the vulnerabilities but also on the strengths of the target (it is recommended to avoid / erode the strong points and exploit the vulnerabilities).

2. In the next stage the ***target analysis*** is carried out (*SWOT* analysis and *structural* analysis), aiming to identify the vulnerabilities and the key operational variables that drive the aggressor's actions.

The SWOT analysis shows the target's vulnerabilities, which, as we have said, will become targets for the aggressor. Vulnerabilities lead to a second selection of actions which the aggressor has the opportunity and must apply to the target in order to achieve his goal. Therefore, the outcome of the SWOT analysis undergone on the target decisively determines the set of aggressions addressing the target and, in addition to the results of the structural analysis, contributes to the crystallization of the strategies of combining them to maximize the effects (especially the results of the *strengths – opportunities* and *threats – weaknesses* relation analysis).

The *structural analysis*[4] of the target actor describes its status by presenting its characteristics as system variables and their relationships,

[3] N.A.: *MACTOR* stands for *Matrix of Alliances and Conflicts: Tactics, Objectives and Recommendations*. The method was presented in details by Michel Godet in *From anticipation to action – a handbook of strategic prospective*, United Nations Educational, Scientific and Cultural Organization, Paris, 1994, p. 105. I also present it, in an adapted form, in the article „The prospective analysis of strategic relations between geopolitical actors in the contemporary security environment - the MACTOR method", Internatinal Conference *Strategies XXI – Strategic Changes in Security and International Relations*, organized by Defence and Security Faculty and Doctoral School from „Carol I" National Defence University, April 14-15, 2016, vol. 1, pp. 62-72, available at https://www.strategii21.ro/index.php/ro/conference-proceedings.

[4] N.A. The *MICMAC* method (*Matrice d'Impacts Croisés – Multiplication Appliquée à un Classement*) was invented in 1973 by Michel Godet şi J.C. Duperrin. I also present it, in an adapted form, in the article „*Structural analysis of hybrid aggression target*", Internatinal Conference *Strategies XXI – Strategic Changes in Security and International Relations*, organized by Defence and Security Faculty and Doctoral School from „Carol I" National Defence University, April 06-07, 2017, vol. 1, pp. 87-94, available at https://www.strategii21.ro/index.php/ro/conference-proceedings.

as well as by identifying the relevant aspects capable of justifying possible strategies of the aggressor that cannot be inferred intuitively. It should be specified that the input variables are, first, the target's vulnerabilities determined from its SWOT analysis. In addition to this product of descriptive nature, the results highlight the key variables through which the aggressor can influence the dynamics of the target states so as to distort it. It should not be forgotten that "*one of the main objectives pursued by hybrid threats is the destabilization of the government and the main institutions of the opponent, thereby creating chaos and vacuum of power*."[5] Also, the structural analysis of the target actor results in conclusions about its stability, deduced from the system variables arrangement in the *Direct relationships Chart* and the *Direct and Indirect Relationship Chart*. Relationship charts represent "maps" of the influences and dependencies among the factors that define the target actor and highlight those (*key variables*) the aggressor has to exploit to generate significant perturbations in the system. The factors will prioritize the targets aimed by the actions that make up the hybrid aggression, in an effect based configuration. The products of structural analysis are qualitatively dependent on the objectivity of determining the system variables and the relationships between them.

With the help of the target's structural analysis and the SWOT analysis results, the aggressor can determine a "map" of the necessary effects to be generated on the target for exploiting its vulnerabilities and destabilizing it. More than anything, the aggressor seeks to control the effects of his actions in order to combine and focus them on the target. The aggressor must always keep in mind that the final result is the configuration of a set of actions that, by integrating their effects, lead to achieving the goal, that is to impose its own will on the target without destroying it and without being sanctioned in accordance with international law.

3. Next, ***cross-impact analysis***[6] ***of aggressions*** gives an image of their interdependence, taking into account the conditional probability between them. Applying the method created by Michel Godet (1974) involves compiling (for the aggressor) a cross-impact matrix on the aggressions it can apply to the target, considering the two criteria: the aggressor's capabilities and the target's vulnerabilities. This is a square shape matrix ($\mathbf{A}_\mathbf{n}\times\mathbf{A}_\mathbf{n}$), where $\mathbf{A}_\mathbf{1}, \dots, \mathbf{A}_\mathbf{n}$ represents the actions of the aggressor. The elements of the matrices are in the form $\mathbf{a}_{\mathbf{i/j}}/\mathbf{a}_{\mathbf{i/\bar{j}}}$, where:

- $\mathbf{a}_{\mathbf{i/j}}$ represents the probability of manifestation of the threat $\mathbf{A}_\mathbf{i}$ if $\mathbf{A}_\mathbf{j}$ is manifested
- $\mathbf{a}_{\mathbf{i/\bar{j}}}$ represents the probability of manifestation of the threat $\mathbf{A}_\mathbf{i}$ if not $\mathbf{A}_\mathbf{j}$

Considering the hybrid aggression as a complex of actions with different probability of occurrence, one can calculate the probability that the aggressor generates all possible combinations in the operational environment. For efficiency, one can use the *Smic*[7] application developed by *Heurisco*. Interpretation of the cross-impact analysis results also involves identifying conclusions that complement the results obtained in the stage of determining the strategies of actors present in the operational environment (step 3). Specifically, the conclusions of cross-impact analysis of threats provide valuable information in creating the connections between the actions that make up the aggressor's strategy and the objectives it pursues, in light of the effects it generates.

Configurations of hybrid aggressions are ordered in descending order regarding the probability of occurrence. Thus, the result provides the most likely combinations of actions the aggressor is able to deploy to generate effects on the target. In view of the hybrid threat definition, it is obvious that, in its ideal and complete form, it contains in appropriate proportions and in a coherent manner all the types of aggression that the

[5] Valery Gherasimov, "Value of science in prediction (translated from Russian)", *VPK* Magazine, no. 8(476), February-March 2013, available at http://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf.

[6] Michel Godet, *From anticipation to action – a handbook of strategic prospective*, United Nations Educational, Scientific and Cultural Organization, Paris, 1994, p. 142.

[7] *Smic* software is available at http://en.laprospective.fr/methods-of-prospective/softwares/62-smic-prob-expert.html.

aggressor is able to apply to the target. The art of it is to identify the strategy in which aggressions are applied so as to produce the maximum effect on the target. This activity takes place in the following step.

*4. **Configuring hybrid aggression*** (temporally and spatially) ***and planning the actions*** that make it up is the most important step. After determining the best components of the hybrid aggression, its configuration involves determining the proportions, resources, place, succession and moments when aggressions, as manifestations of threats, are applied so as to produce the maximum effect on the target. In order to determine the most effective way of action, different decision-making methods can be used in support. One of them is the *ORANetScenes*[8] software, which considers as inputs the set of instruments, objectives, strategies as:

- *Instruments* – instruments available to the aggressor.
- *Objectives* – the key vulnerabilities of the target.
- *Strategies* – hybrid aggression configurations.

The application has the capability to display a graphical representation of the *instruments-strategies-objectives* triad and to determine which strategies (in this case, hybrid aggression configurations) are most efficient (use fewer resources to achieve the goals) and more effective (lead to the achievement of as many of the proposed objectives as possible). In addition to specifying all instruments, objectives, and strategies, the user must also enter data related to the *instruments-strategies* (which means are used to apply each configuration of hybrid aggression) and the *strategies-objectives* relationships (what goals are achieved by each aggression of the hybrid type).

Each configuration can be represented in the form of a graph that highlights the causal relationships (closely related to the effects that each generates) that are established between the actions that make them up. Thus, for an analyzed hybrid aggression, the nodes of the graph represent the actions, and the connections between the nodes represent the existence of a causal relationship between them (elements of the square matrix $\mathbf{A_n}\times\mathbf{A_n}$ in the cross-impact analysis). Thus, the craftsman of hybrid aggression has the possibility to estimate (and control) the resulting effect of each hybrid configuration by analyzing how the effects of each component are integrated in the whole picture.

The configurations obtained are the essence of hybrid aggression planning. They can materialize through an "operational design" representation, i.e. a representation of the chronological succession of the component actions (with the necessary resources and their resulting effects) and the achievement of the objectives pursued by the aggressor. The aggressor can also make a convenient configuration selection using any criterion, which may be the probability, the time available for preparing and executing actions, etc. Subsequently, he will develop this product in a plan, achieving the connection in the temporal and spatial dimension between resources and objectives through actions (aggressions) and effects.

5. The seventh stage consists of ***interpreting the results of the threat analysis***. It should be noted that the developed method does not provide a quantified result with regard to the resulting effect of hybrid aggression. The compound effect of a set of aggressions that manifest (partially) simultaneously on a target is extremely unpredictable, and applying mathematical methods to determine the amount of interference between them could lead to misleading results. However, after determining the hybrid aggression configurations, through their structural analysis, an effect map can be determined and compared to the "image" (achieved in the initial stages) presenting the effects needed to successfully exploit the target's vulnerabilities. Thus, considering the means available to the aggressor and the actions it may undertake to exploit target's vulnerabilities, by adapting the MICMAC method of structural analysis, one can determine the key components of hybrid

[8] *ORANetScenes* software is available at http://oranetscenes-st-iw-32.updatestar.com/.

aggression (using actions instead of operational variables) and how they facilitate (influence) or are favored (dependent) in relation to the other components. The results also lead to conclusions that can be used to identify the most probable components of hybrid aggression, as well as their time course (successive/simultaneous, periodic/permanent). Regarding the stability/instability of hybrid aggression (as a system) the MICMAC method offers the possibility to determine its vulnerabilities from which derive ways of countering it, extremely useful information in determining the target's actions.

Conclusions

Throughout the operational environment, hybrid threats manifest themselves in a configuration of great complexity, always different, tailored to the vulnerabilities of the target actor and in a manner that often produces an imbalance effect that exploits its capabilities in all areas, diminishing its power to react. Thus, countering the hybrid threat becomes one of the most complex issues in achieving the security of the world's actors at the beginning of the 21st century. Consequently, the conflict in which hybrid aggression is present is no longer a matter of national defense, but becomes a national security issue.

The measures and actions countering the hybrid threat must start before it materializes into aggression, they must be designed and deployed in a proactive manner. Otherwise, the target actor will encounter major difficulties in configuring the answer, burdens that will exponentially escalate as its power diminishes. The augmentation of the capabilities needed to counter the hybrid threat can be done by anticipating crisis situations, by properly preparing the force, and by deploying efficient and effective actions to formulate the appropriate response. These sequences must be connected to each other through an efficient planning process that must be carried out in a comprehensive manner at all levels of the parties involved in the conflict. A useful tool is the scenario method, which provides a flexible and controlled framework, a "laboratory" that allows the articulate use of a variety of algorithms and procedures to identify the optimal response and, also, to train and evaluate the forces.

Depending on the method of application, the scenario method can trigger the operational planning process or support it throughout its entire evolution. The purpose of using it is to eliminate uncertainty or, at least, to establish controllable limits around the uncertainties generated in the hybrid operational environment and to concentrate planners' efforts on solving the problem. In addition, the use of the scenario method in the planning process facilitates the use of advanced operational research procedures that, in conjunction with modeling and simulation, contribute to the creation of viable and valid plans to generate a flexible and efficient response capability.

BIBLIOGRAPHY:

1. ARCADE, Jaques; GODET, Michel; MEUNIER, Francis; ROUBELAT, Fabrice, *Structural analysis with the MICMAC method & Actors' strategy with MACTOR method*, AC/UNU Millennium Project - Laboratory for Investigation in Prospective and Strategy (LIPS), Paris, 2003.

2. DUŢU, Petre, *Ameninţări asimetrice sau ameninţări hibride: delimitări conceptuale pentru fundamentarea securităţii şi apărării naţionale*, "Carol I" National Defence University Publishinghouse, Bucharest, 2013.

3. GHERASIMOV, Valery, "Value of science in prediction (translated from Russian)", *VPK* Magazine, no. 8(476), February-March 2013, available in Russian at http://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf.

4. GLENN, Russel, "Thoughts on <Hybrid> Conflict", *Small Wars Jurnal*, Small Wars Journal LLC, March 2, 2009, available at http://smallwarsjournal.com/jrnl/art/thoughts-on-hybrid-conflict

5. GODET, Michel, *From anticipation to action – a handbook of strategic prospective*, UNESCO, Paris, 1994.

6. GORDON, Theodore Jay, *Cross-Impact Method*, AC/UNU Millennium Project, Paris, 1994.

7. HOFFMAN, Frank, Hybrid *Threats: Reconceptualizing the Evolving Character of Modern Conflict*, Institute for National Strategic Studies, National Defense University, NDU Press, *Strategic Forum* No. 240, April, 2009.

8. HOFFMAN, Frank, MATTIS James, "Future Warfare: The Rise of Hybrid Wars", *Proceedings Magazine*, vol. 132/II/1,233, US Naval Institute, November, 2005.

9. HOFFMAN, Frank, "Hybrid vs. compound war", *Armed Forces Journal*, October 1, 2009, available at http://armedforcesjournal.com/hybrid-vs-compound-war/.

10. OMRAN, Ahmed; KHORISH, Motaz; SALEH, Mohamed, *Structural Analysis with Knowledge-based MICMAC Approach*, International Journal of Computer Applications, Vol. 86, No. 5, 2014, available at https://pdfs.semanticscholar.org/9515/b310ab104da6f2c2116fb6a42e19ade6adb5.pdf.

CONCEPTUAL APPROACHES TO CYBERSPACE IN NATO, EU AND ROMANIA

*Mirela ATANASIU, Ph.D**

Concomitantly with the expansion of the use of information and communication technologies in all areas of social life, including military, organizations and states across Europe have noted the need to raise awareness of cyberspace risks and to act in order to prevent and combat them. For example, on the one hand, NATO - a political-military organization - has included cyberspace among its operational areas, considering it a space of battle, besides the three already traditional - air, land and naval. On the other hand, the European Union - a political and economic organization - is more concerned with cyber security and cybercrime, being aware that networking is essential to maintaining the online economy and ensuring the prosperity of its states and citizens. Also, at the level of Romania, a series of initiatives have been launched that target the so sensitive digital space.

In the present paper, without pretending to have an exhaustive approach, we wish to present the current conceptual framework of cyber security at the Euro-Atlantic, European and national levels and, very briefly, some converging initiatives in the field.

Keywords: cyber security, vulnerability, war dimension, NATO, EU, Romania.

Introduction

In the last decades, information technology has developed a lot. From a purely administrative tool that helps to optimize bureaucratic processes, it has become a strategic tool used in industry, transport, medicine, biology, administration, the army, etc., in the context in which, before September 11, 2001, the risks and the cyber security challenges were discussed only in small groups of technical experts. But, from that day, it became clear that the cyber world is attracting serious security challenges to increasingly interdependent societies.

At present, companies, states and international organizations are involved in the ongoing activity of counteracting risks, threats and vulnerabilities to the security of the digital world. For example, state or non-state actors may exploit the increased complexity and connectivity of cyber-critical infrastructure networks (banking systems, public transport systems, power systems, etc.) operated and controlled by information and communications technology, with the potential to cause material damage and major financial losses and thus endanger the security, economy, public safety of some states and the welfare of their citizens.

1. Cyberspace - the fourth Euro-Atlantic dimension of war

Throughout history, military conflicts have varied in sphere and complexity, strategy and tactics, but a constant element of all these military clashes remains the need for an actor to mobilize his infrastructure and capacity to attack another in order to obtain victory. The same

Mirela ATANASIU, PhD is Senior Researcher within the Centre for Defence and Security Studies/"Carol I" National Defence University, Bucharest, Romania. Email: atanasiu.mirela@unap.ro

applies to the cyber tool that directly relates to the ability of an opponent to use own informational capabilities in order to exploit the vulnerabilities of their opponents. Likewise, similar to the armed conflicts, and in the cyber war, each opponent uses different tactics, techniques and procedures to gain supremacy in combat, and logistics, communication, and battlefield knowledge become essential to reach the ultimate goal – to defeat the opponent.

Cyber threats are part of the hybrid war[1]. They can also be misleading and toxic to civilians, states or states' groups. Threats have the potential to damage, destroy or eliminate the operation of critical infrastructure that is vital to the well-being of some states, because by using advanced IT tools, state or non-state interest groups can control power networks and power systems, computerized industrial conglomerates, electronic payment systems, private data of civilians and the intellectual property of national or international institutions or organizations.

NATO is among the international organizations that have realized the extent of the impact and consequences of this type of threat. In this respect, in a public document, it is stated that "cyber-attacks are becoming more frequent, sophisticated and harmful. The Alliance is confronted with an environment where cyber security threats develop exponentially. State and non-state actors may use cyber-attacks in the context of military operations. [...] NATO must be prepared to defend its networks and operations against the cyber threats and increasingly sophisticated attacks it confronts"[2]. But awareness has not only been at the speech level, with the organization reacting proactively to keep pace with the accelerated dynamics of virtual network threats.

One of the many actions in this regard is that at the time of the NATO Summit in Wales in September 2014 when, in the context of discussing the improvement of the organization's capabilities to combat new or old threats to Euro-Atlantic security, Member States agreed the implementation of "a Defence Planning Package including a series of priorities in the areas of strengthening training and exercises programs; command and control, including for consumptive air operations; Intelligence, Surveillance and Recognition (ISR); NATO's defence capacity against ballistic missiles, [...] cyber defence"[3]. So, the key areas of NATO included cybernetic.

On this occasion, NATO has adopted a reinforced cyber defence policy and an action plan that has been approved by the Member States. Also, by the Alliance's cyber security policy there is stated that cyber defence is one of the main tasks of collective defence, an essential priority identified at the organizational level being the protection of communications and information systems owned and operated by NATO.

Subsequently, at the NATO Summit in Warsaw in 2016, NATO Heads of State and Government have recognized cyberspace as "an operational area, apart from the traditional ones - air, land and naval"[4]. The reason for this recognition was that "the treatment of cyberspace as an operational domain will allow the Alliance to better protect its missions and operations by focusing more on military training and planning"[5], while providing "a more conducive framework for managing resources, abilities, capabilities and coordinating decisions"[6]. The main instrument for implementing this framework is the Enhanced NATO Policy on Cyber Defence, corroborated with NATO's cyber defence strengthening capability initiative with up-to-date technologies.

[1] ***, *Cyber defence,* North Atlantic Treaty Organization, February 17, 2017, URL: http://www.nato.int/cps/on/natohq/ topics_78170.htm, accessed on 02.05.2017.

[2] ***, *NATO Cyber Defence*, North Atlantic Treaty Organization, URL: http://www.nato.int/nato_static_fl2014/ assets/ pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf, accessed on 06.05.2017.

[3] ***, *Wales Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales*, September 5, 2014, http:// www.nato.int/cps/ic/natohq/official_texts_ 112964.htm, accessed on 05.05.2017.

[4] ***, *NATO Cyber Defence*, Fact Sheet, North Atlantic Treaty Organization, July 2016, http://www.nato.int/ nato_ static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf, accessed on 08.05.2017.

[5] *Ibidem*.

[6] *Ibidem*.

Until cyberspace was declared as a new dimension of warfare, the Alliance's IT security has gone through a route divided by specialists[7] in three stages:

- The first took place when IT security was treated more as a technical challenge that had to be confronted both on a collective basis by NATO means and individually by each of its member states. Thus, the initiative was seen as securing activity of the communication and information technology (ICT) infrastructure used by NATO with the collective contribution of its Member States, and the securing activity of national ICT networks was carried out at the national level of the Member States;
- The second stage was initiated when cyber issues became an important political topic (the process was initiated during the Riga Summit in 2006 and was subsequently intensified following the cyber-attacks against Estonia in 2007);
- The third stage, which is still underway, began in 2014 at the NATO Summit in Wales, when IT security was declared as a strategic challenge of common interest to Alliance members, requiring a coordinated response from the whole Euro-Atlantic security community and of all NATO member states, even questioning "the invocation of Article 5 of the Washington Treaty, if cyber-attacks reach a threshold that threatens Member States' prosperity, security and stability and the Euro-Atlantic dimension"[8], all in all. Indeed, at present, NATO's cyber security priorities are two, namely, protecting its own Alliance-specific IT networks and assisting Member States in developing their own cyber capabilities. The activities circumscribed to these priorities are addressed, this time together, and not separately.

At the moment, the diversity of means wherewith cyber capabilities can be used is one of the greatest challenges for NATO in understanding its own role in cyber defence[9]. Two main types of cyber-attacks are particularly relevant to NATO's role in the cyber field. Firstly, cyber-espionage - from a strategic or operational level - can compromise the confidentiality of information and communications systems, with the ability to reveal secret and sensitive information to the opponents. Secondly, cyber sabotage can cause significant material damage, especially when it comes to critical infrastructure such as power or transport networks or databases that an opponent can attack by denying access, moving or modifying them with potential to create major damage to the target and even undermine the process of assisted (or not) command and control decisions.

2. The cyber threat and the internal security of the European Union

Cyber security is also a major concern of the European Union. In this context, in the framework of the Union there is work on several directions to ensure that this security dimension is safeguarded, from the improvement of Member States' capabilities internally, to the implementation of international cooperation on cyber security and cybercrime. This is a major activity in the context of the awareness over the fact that securing the network and information systems in the EU territory is essential for the smooth development of the trade in the virtual environment and for providing the prosperity of citizens and states.

In 2004, the European Network and Information Security Agency (ENISA) was established to support the implementation of relevant EU law in the field, at Member State level, and to improve the resilience of Europe's

[7] Joanna ŚWIĄTKOWSKA, „NATO's Road to Cybersecurity – towards bold decisions and decisive actions", in *NATO Road to Cybersecurity*, The Kosciuszko Institute, Kraków, Poland, 2016, p. 5, http://www.ik.org.pl/wp-content/ uploads/nato_road_to_cybersecurity_the_kosciuszko_institute_2016.pdf, accessed on 11.05.2017.

[8] ***, *Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales,* Press Release, North Atlantic Treaty Organization, September 5, 2014, point 72, http://www.nato.int/cps/en/natohq/official_texts_112964.htm#cyber, accessed on 11.05.2017.

[9] ***, „NATO: changing gear on cyber defence", in *NATO Review Magazine*, http://www.nato.int/docu/Review/2016/Also-in-2016/cyber-defense-nato-security-role/EN/index.htm, accessed on 10.05.2017.

critical information infrastructures and networks. Thus, ENISA has launched a first definition of a minimum set of capabilities that a Computer Emergency Response Team (CERT) responsible for protecting critical information infrastructure (CIIP) in the EU Member States must possess, an initiative materialized in 2009 through the document "Baseline capabilities for national/governmental CERTs (Part 1 Operational Aspects)". Such a document was also translated in Romanian in December 2010 with the intention of establishing such a team at national level.

As a result of the European perception of the importance of the cyber domain in the context of ensuring security and prosperity space, an important document is the *European Union's Cyber Security Strategy from 2013* which "sets out the EU's strategy for preventing and responding to disruptions and attacks that affect Europe's telecoms network"[10], as a result of the finding that "in recent years ... the digital world brings enormous benefits but is at the same time vulnerable. The number of cyber security incidents, whether intentional or accidental, increases at an alarming rate and could disrupt the provision of essential services that we consider to be self-evident, namely water or electricity supply, healthcare or mobile telephony services. Threats can come from diverse sources – such as criminal, terrorist attacks, politically motivated or commanded by opponents (author's note, state and non-state actors), as well as natural catastrophes or unintentional mistakes"[11].

Also in the body of the *European Commission Communication to the European Parliament, the European Council, the Economic and Social Committee and the Committee of the Regions in Strasbourg on 28 April 2015*[12] was set the *European Agenda on Security for 2015-2020*, "with the role to support Member States' cooperation in combating security threats and intensifying common efforts in the fight against terrorism, organized crime and cybercrime"[13]. So, the Agenda clearly shows the three security threats that have lately combined with serious international outcomes, which may become a major issue at the European level over time.

The European Union's Cyber Security Strategy and the *European Agenda on Security* provide the overall strategic framework for EU initiatives on cyber security and cybercrime. *The Digital Single Market Strategy* recognizes the importance of trust and security in the digital space. A study shows that by completing the digital single market, the EU could grow its economy by almost € 415 billion a year and create hundreds of thousands of new jobs[14]. But, in order for Europeans to agree on the implementation of such new digital technologies and their widespread services within peoples' societies, they must receive signals that will increase their confidence in a high level of cyber security at European level.

Given these gaps over the level of security accepted by the European Community to increase confidence in the use of information technology and communications, the European Commission's main cyber security goals include[15]:

- *Enhancing cyber security capabilities and cooperation* in order to bring digital security capabilities to the same level of development in all EU Member States and to ensure that exchanges of information and cooperation

[10] ***, *Improving cyber security throughout the EU*, Council of the European Union, 2013 (In Romanian: *Îmbunătățirea securității cibernetice în întreaga UE*, Consiliul Uniunii Europene, 2013), URL: http://www.consilium.europa.eu/ro/policies/cyber-security/, accessed on 14.05.2017.

[11] ***, *The European Union's cyber security strategy: an open, secure and secure cyberspace*, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, JOIN/2013/01 final (In Romanian: *Strategia de securitate cibernetică a Uniunii Europene: un spațiu cibernetic deschis, sigur și securizat*, Comunicare Comună către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor, JOIN/2013/01 final).

[12] ***, *The European Agenda on Security*, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Strasbourg, 28.04.2015 COM (2015) 185 final.

[13] ***, *Commission takes steps to strengthen EU cooperation in the fight against terrorism, organized crime and cybercrime,* Strasbourg, 28 April 2015, p. 1.

[14] ***, *Cybersecurity,* Digital Single Market, https://ec.europa.eu/digital-single-market/en/cybersecurity, accessed on 10.05.2017.

[15] *Ibidem*.

are effective, including at cross-border level. In this area, the Directive on Security of Network and Information Systems (the NIS Directive) is the main instrument supporting cyber resilience in Europe;

- *Transforming EU into a strong IT security player* by promoting the competitive advantage of the political and economic organization in the field of cyber security in order to ensure that European citizens, enterprises and public administrations have access to the latest digital security technology interoperable, competitive, trustworthy and respecting the fundamental rights of individuals, including the right to privacy;
- *Integrating IT security into EU policies*, especially in policies related to new technology and emerging sectors, such as connected machines, smart grids and the Internet of Things (IoT).

Following the implementation of the Cybersecurity Strategy of the European Union in 2013, the Network and Information Security Platform (NISP)[16] was created in public-private partnership to help stakeholders to identify best practices in cyber security for information security and Information and Communication Technologies (ICT) security, creating favourable market conditions for the development and adoption of safe technological solutions.

Subsequently, in July 2016, the *Directive concerning measures for a high common level of security of network and information systems across the Union* was adopted, which states that "it should be created a cooperation group composed of representatives of the Member States, the European Commission and the European Network and Information Security Agency to support and facilitate strategic cooperation between Member States on network and information security"[17].

Also, in September 2017, the European Commission started the revision of the European Cyber Security Strategy of 2013 issuing a Working Document presenting an assessment of it[18]. The new EU cybersecurity strategy is aimed to be adopted by 2019. Concomitantly, the same European body initiated a proposal for a Regulation on ENISA[19] stipulating guidelines of its following mandate which will start in 2020[20] in order to align it with the new European Computer Security Framework.

3. National Cyber Security Framework

Romania cannot ignore the developments in cyber matters nor does it, as it is emphasized in its strategies and policies related to the field. Thus, in the *National Defence Strategy for the period 2015-2019 - A strong Romania in Europe and the world* - among the medium and long term trends with potential to affect the global security environment, "cyber-attacks"[21] are also identified. In the same

[16] ***, *NIS Platform. Network and Information Security Risk Management Organisational Structures and Requirements*, Final Draft, 22.05.2015, p. 3, https://resilience.enisa.europa.eu/nis-platform/shared-documents/ 5th-plenary-meeting/chapter-1-nis-risk-management-organisational-structures-and-requirements-v2/view, accessed on 21.02.2017.

[17] ***, *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union published in the Official Journal of the European Union, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG.*

[18] ***, *Commission Staff Working Document Assessment of the EU 2013 Cybersecurity Strategy*, European Commission, Brussels, 13.9.2017, SWD(2017) 295 final, https://ec.europa.eu/transparency/regdoc/rep/other/SWD-2017-295-F1-EN-0-0.PDF.

[19] ***, *Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act")*, European Commission, Brussels, 13.9.2017 COM(2017) 477 final 2017/0225 (COD), available online at: https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-477-F1-EN-MAIN-PART-1.PDF,accessed on 12.02.2018.

[20] ENISA is the single European agency with fixed term mandate (7 years). The ongoing mandate started in 2013 and ends in 2020. See details: *Ibidem*, p. 6.

[21] ***, *National Strategy for Country's Defence for 2015-2019 - A strong Romania in Europe and the world* (in Romanian: *Strategia Națională de Apărare a Țării pentru perioada 2015-2019 – O Românie puternică în Europa și în lume)*, Administrația Prezidențială, București, 2015, p. 11.

strategic context, it is realized that "cyber-threats launched by hostile, state or non-state entities, on information infrastructures of strategic interest of public institutions and companies, cyber-attacks executed by cybercrime groups or cyber-attacks launched by extremist groups of hackers directly affect national security"[22]. As a result, national security objectives include, among other things, "strengthening the security and protection of critical infrastructures - energy, transport and cyber -, as well as food security and the environment"[23]. Subsequently, within the same document, it is established as an action line "the provision of mechanisms to prevent and counteract cyber-attacks on information infrastructures of strategic interest, associated with the promotion of national interests in the field of cyber security"[24]. Therefore, these elements presented in the Strategy highlight the political awareness of the presence of cyber threats, the will to act to combat this threat and to initiate the implementation of a normative framework and the designation of related prevention bodies that ensure the security balance in the Romanian virtual space, at least as regards the protection of critical infrastructures and strategic information circulated in this fluid environment.

By the Decision of the Supreme Council for National Defence no. 16/2013 and Government Decision no. 271/2013 there was approved the *Cyber Security Strategy of Romania*, which establishes the conceptual, organizational and action framework necessary to ensure cyber security and aims to protect cyber infrastructures in line with new concepts and policies in the field of cyber defence elaborated and adapted at NATO level and of the European Union.

In this document, on the one hand, cyber security is defined as "the normality status resulting from the application of a set of proactive and reactive measures that ensure the confidentiality, integrity, availability, authenticity and non-repudiation of information in electronic format, of public and private resources and services in cyberspace"[25]. Cyber defence, on the other hand, is defined as the sum of "actions undergone in the cyber-space in order to protect, monitor, analyse, detect, counteract aggressions, and provide the appropriate response against threats on cyber-specific infrastructures specific to national defence"[26]. A distinction is therefore made between the types of cyber-security and cyber-defence specific activities and the generic measures taken to ensure the security framework for communications and information technology infrastructures in general and cyber-specific actions to ensure national defence.

According to Government Decision no. 271/2013, "the Ministry of Information Society (Ministry of Communications and Information Society, author's note) the responsible public authorities have the obligation to carry out the objectives and the directions of action provided in the Cyber Security Strategy of Romania and in the Plan of action at national level regarding the implementation of the National Cyber Security System, in compliance with the legal provisions in force"[27]. Also, in the same document, there are explained a number of other collocations related to cyber security and defence, such as "cyber threat", "cyber-attack", "cyber hazard", "cyber terrorism", "cyber espionage", "cybercrime", "vulnerability in cyberspace", "security risk in cyberspace", reaching to the identification of four major categories of cyber challenges for national security: the first two largely associated with states, namely cyberwar and economic espionage, and the latter two, largely associated

[22] *Idem*, pp. 14-15.

[23] *Idem*, p. 9.

[24] *Idem*, p. 20.

[25] ***, *Decision no. 271/2013 for the approval of the Cyber Security Strategy of Romania and the National Action Plan on the Implementation of the National Cyber Security System* published in the Official Gazette no. 296, Part I, 23.05.2013, p. 7 (in Romanian: *Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică* publicată în Monitorul Oficial nr. 296, Partea I, 23.05.2013, p. 7), https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf, accessed on 26.05.2017.

[26] *Ibidem*.

[27] *Ibidem*.

with non-state actors - cybercrime and cyber terrorism.

In Romania, according to the Cyber Security Strategy, coverage of the domain is ensured by the *National Cyber Security System* (NCSS), which is “the general framework of collaboration bringing together public institutions and authorities with responsibilities and capabilities in the field to coordinate actions at the level of national network for ensuring the Romanian cyberspace, including by cooperation with the academic and business environment, professional associations and non-governmental organizations”[28].

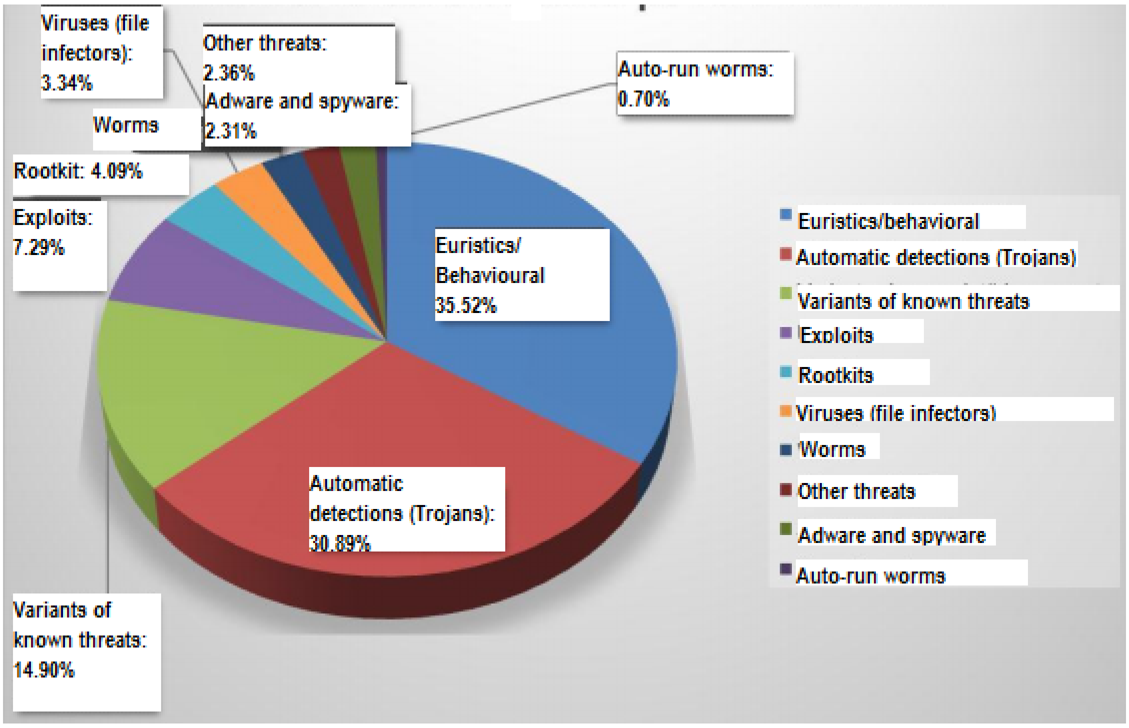


Figure no. 1: The distribution of computer threats in the first 6 months of 2013

Sources: https://www.cert.ro/vezi/document/amenintari-cibernetice-la-adresa-utilizatorilor-romani, accessed on 25.05.2017.

In the System’s framework, the Romanian National Computer Security Incidents Response Team (CERT-RO), based on the EU-promoted model, ensures “the development and dissemination of public policies to prevent and counteract incidents within cyber infrastructures, in regard to the competence area”[29].

Therefore, CERT-RO is the specialized organizational entity that has the capability to prevent, analyse, identify and respond to cyber incidents. At CERT-RO level, the procedural and technical disparities in the national cyber infrastructure are analysed[30]. CERT-RO is also a national contact point with similar foreign structures.

This organizational entity issues a series of documents that help raise awareness of cyber security risks and disseminate the security culture In the cyber domain at a national level. These documents include guides, good practice manuals, data management procedures, cyber protection ideas and tips, reports, and

[28] *Idem*, p. 12.

[29] ***, *CCS146 – Securitatea Cibernetică – Securitatea Rețelelor și Sistemelor Informatice: „Scenarii și soluții privind soluționarea incidentelor de securitate – gestionarea incidentelor la nivel national cu potential impact pe scară largă”*, project elaborated in the framework of MSI Sectoral Plan, 2015, p. 26, https://www.comunicatii.gov.ro/wp-content/ uploads/2016/02/CyberSec_nov2015.pdf, accessed on 23.05.2017.

[30] Romanian National Computer Security Incident Response Team (In Romanian: Centrul Național de Răspuns la Incidente de Securitate Cibernetică), http://internship.gov.ro/informatii/centrul-national-de-raspuns-la-incidente-de-securitate-cibernetica/#null, accessed on 24.05.2017.

documentation on the types and forms of cyber threats that are emerging. Such a document is the "Cyber Threats to Users in Romania" Report, conducted for the first half of 2013 by Bitdefender, which showed that "in the first half of 2013, the most important threats with malware in Romania were Trojans, followed by variants of other already known threats, but reused by attackers by specific techniques"[31].

In the same Report, a series of useful tools for confidentiality protection, a list of cyber security centres against threats, and a range of government resources that can support individuals, companies, and state bodies in cybercrime prevention are presented.

Currently, Romania does not have a cyber security law, but in recent years efforts have been made in this direction. A first initiative was in 2014, but was rejected in the Senate of Romania, following objections of unconstitutionality accepted by the Constitutional Court, by Decision no. 17/21 January 2015 published in the Official Gazette no.79 of 30.01.2015[32].

Subsequently, at the end of January 2016, the Ministry of Communications launched a public debate on another draft Law on Cyber Security of Romania, improved by considering the criticism brought by the previous ruling of the Romanian Constitutional Court (RCC) on the objection of unconstitutionality as a result of violation of the constitutional provisions on the rule of law and the principle of legality, as well as those on intimate, family and private life, respectively the secrecy of correspondence[33]. In February 2017, the Minister of Communications and Information Society stated that "The Cyber Security Law is not among the priorities ... and will not go further to the Parliament ..."[34], justifying this position by the existence of the European Directive no. 1148/2016, *NIS - Networking Information Security*, adopted in Parliament, which the official considers that it already covered the field of cyber security as presented in the related draft law. Personally, I believe that the issuance of this law is necessary and does not overlap with the European directive.

Conclusions

Cyber threats do not take into account the national, European or international geographic boundaries because computer systems are interconnected in networks beyond these levels, so the national computer system is interconnected with the European and NATO ones. This causes a minor vulnerability of an information microsystem to create, as a result of the "network effect", major problems for a larger part or a system as a whole, which requires international consistency in the setting of preventive and combating regulations and measures for them.

In this respect, Romania − a member of NATO and the EU - must rally its cyber security policy to the policies of both organizations. On the one hand, it must work towards continuing review of strategic documents on cyber security and, on the other hand, developing national cyber capabilities, therefore to be compatible and secure to the level of the others in the organizations they are part of.

As we have presented in this paper, cyber concerns are real at all approached levels: Euro-Atlantic, European and national. However, there are some gaps between the ratio of intensification and diversification of cyber threats and the speed of implementation of appropriate preventive

[31] ***, *Raport. Amenințări cibernetice la adresa utilizatorilor din România*, BitDefender, 2016, p. 6, https://www.cert.ro/vezi/document/amenintari-cibernetice-la-adresa-utilizatorilor-romani, accessed on 25.05.2017.

[32] *Proiect de lege privind securitatea cibernetică a României*, https://www.senat.ro/Legis/Lista.aspx?cod=18494, accessed on 22.05.2017.

[33] *Cosmoiu (SRI): Noua Lege a securității cibernetice nu are un caracter intruziv*, Agerpress, June 14, 2016, https://www.agerpres.ro/cybersecurity/2016/06/14/cosmoiu-sri-noua-lege-a-securitatii-cibernetice-nu-are-un-caracter-intruziv-11-25-15, accessed on 23.05.2017.

[34] *Jianu (MCSI): Legea securității cibernetice nu se află printre prioritățile mele; România trebuie să implementeze legi pe baza Directivei NIS*, Agerpress, February 15, 2017, https://www.agerpres.ro/economie/2017/02/15/jianu-mcsi-legea-securitatii-cibernetice-nu-se-afla-printre-prioritatile-mele-romania-trebuie-sa-implementeze-legi-pe-baza-directivei-nis-11-36-50, accessed on 26.05.2017.

measures at the level of the information and communication systems, and this is felt on all mentioned levels, not only at national level.

We believe that in order to ensure a high level of security of the cyberspace among a number of organizations of states such as the EU or NATO, the main role lies with the national states, and a bottom-up approach is needed, at least in terms of the provision with performing information and technology communications, more resilient to vulnerabilities and threats.

For this, it is necessary to invest heavily in such systems, especially since most technologically advanced states consider cyber capabilities to be a legitimate and necessary part of their set of strategic tools along with diplomacy, economic force and military power. However, this approach raises concerns that, in the near future, we may witness a total war between states, driven into cyberspace. In addition, we notice an occasional interest in the use of cyber capabilities by non-state actors - now with limited evidence of their actual use. In fact, the current experience with the real use of cyber capabilities by states suggests that such capabilities fall under the category of espionage-specific or sabotage-specific instruments, which makes their hiring go beyond simple armed assault. Although there is a certain logic of this argument, it is becoming increasingly clear that some states regard cyber capabilities as an integral part of operational military capability and are not afraid to use them as such even if they are reluctant to recognize publicly such use.

Romania's experience shows that continuous improvement of the relevant rules on cyber security is necessary. At the same time, the dynamics of legislative regulations on cyber security is slower, not only at national level, but also at other higher levels, compared to the dynamics of perpetuation and development of information threats, which can lead to gaps in effective coverage of the domain.

BIBLIOGRAPHY:

1. ŚWIĄTKOWSKA, Joanna, "NATO's Road to Cybersecurity – towards bold decisions and decisive actions", in *NATO Road to Cybersecurity*, The Kosciuszko Institute, Kraków, Poland, 2016.

2. ***, *CCS146 – Securitatea Cibernetică – Securitatea Rețelelor și Sistemelor Informatice: "Scenarii și soluții privind soluționarea incidentelor de securitate – gestionarea incidentelor la nivel national cu potential impact pe scară largă"*, project elaborated in the framework of the MSI Sectoral Plan, 2015.

3. ***, *Commission takes steps to strengthen EU cooperation in the fight against terrorism, organized crime and cybercrime,* Strasbourg, 28 April 2015.

4. ***, *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union published in the Official Journal of the European Union, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG.*

5. ***, *Decision no. 271/2013 for the approval of the Cyber Security Strategy of Romania and the National Action Plan on the Implementation of the National Cyber Security System published in the Official Gazette no. 296, Part I of 23.05.2013* (In Romanian: *Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică publicată în Monitorul Oficial nr. 296, Partea I din 23.05.2013).*

6. ***, *Improving cyber security throughout the EU, Council of the European Union, 2013*

7. ***, *NATO Cyber Defence*, Fact Sheet, North Atlantic Treaty Organization, July 2016.

8. ***, *NIS Platform. Network and Information Security Risk Management Organisational Structures and Requirements*, Final Draft, 22.05.2015.

9. ***, *Raport. Amenințări cibernetice la adresa utilizatorilor din România*, BitDefender, 2016.

10. ***, *The European Union's cyber security strategy: an open, secure and secure cyberspace*, Joint Communication to the European Parliament,

the Council, the European Economic and Social Committee and the Committee of the Regions, JOIN/2013/01 final

11. ***, *The National Defence Strategy of the Country for the Period 2015-2019 - A Strong Romania in Europe and the World,* Presidential Administration, Bucharest, 2015 (In Romanian: *Strategia Națională de Apărare a Țării pentru perioada 2015-2019 – O Românie puternică în Europa și în lume,* Administrația Prezidențială, București, 2015).

12. ***, *The European Agenda on Security,* Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Strasbourg, 28.4.2015 COM (2015) 185 final.

*13. ***, Wales Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales*, September 5, 2014.

*14. ***, Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales*, Press Release, North Atlantic Treaty Organization, September 5, 2014.

15. Agerpress news agency website, www.agerpres.ro.

16. Official website of the European Commission, https://ec.europa.eu.

17. Official website of CERT-RO, https://cert.ro.

18. Official website of NATO, www.nato.int

19. Official website of Romanian Senate, www.senat.ro.

20. Official website of the European Union, www.europa.eu.

MATHEMATICAL MODELS SPECIFIC TO THE MILITARY DOMAIN

*Florentina-Loredana DRAGOMIR, PhD. **

In order to identify the trends in the evolution of some processes, the connections between them, as well as the future implications for the development of the activity, it is necessary to limit the number of alternatives (solutions) regarding the way of conducting events. Starting from the possible alternatives (solutions), we can identify the best, based on certain criteria, techniques, procedures, methods. The process of identifying the optimal variant, in response to certain criteria, involves responsibility and, most of the time, a risk. However, the risk can be diminished by formalizing the decision-making process using mathematical models and methods.

***Keywords**: model, mathematical model, modeling phases, modeling, military model, decision.*

1. Conceptual delimitations

The concept of "model" used in the academic sphere aims at knowing in detail the reality, the process itself, the need for substantiation and decision-making. The model becomes a working tool for assessing the potential effects of decisional alternatives.

Mathematical modeling is the transition from the phenomenon itself to the mathematical relations that characterize the connections between its components as well as the connections with other phenomena. Mathematical modeling is an analytical problem and research experiment of various dynamic processes.

The real basis of mathematical modeling is the isomorphism of the phenomena of nature, thereby understanding a common form of their description through appropriate computational relationships. Hence, it is possible to reduce the study of one of the isomorphic systems to the study of another system, to model the behavior of one system with the help of another. Isomorphism reveals unity, bond, and interaction within determined boundaries, which allows analysis of a process to be done through another, similar in shape and structure, but easier to study. The mathematical model consists of the logical-mathematical relations (formulas, equations, inequalities, logical conditions, operators, etc.) that mirror the quantitative ratios (characteristics of the state of the system, its outputs according to its parameters and inputs, initial and time conditions) of the development of the phenomenon analyzed.

2. Main features of the models

Models have to fulfill the following defining features[1]:

- the more similar the relationship between the two systems (original and model), the greater the possibility of knowing the original through its model;
- as the properties that form the object of the

[1] Gheorghe Ilie, Ion Stoian, Gelu, Alexandrescu, *Modelarea sistemelor şi proceselor*, Editura Universităţii Naţionale de Apărare "Carol I", 2005, p. 41.

Florentina-Loredana DRAGOMIR, PhD. is a Lecturer at the Department of Military Information Systems and Defence Information at the Security and Defence Faculty, "Carol I" National Defence University in Bucharest, Romania. E-mail: dragomir.florentina@myunap

similarity relationship are more important for the two systems, the greater the probability of obtaining true conclusions about the original, inferred by its model;

- if there is a general property in the model that does not appear in the original, then the conclusions deduced from it may be irrelevant to the real system;
- the better known is the connection of the general similarity characteristics of the two systems, the more the conclusions about the original, deduced from its model, are closer to certainty.

A model must meet the following requirements:

- simplicity - necessity to contain only the strict information for the described process;
- flexibility - a feature required by the need to describe, by using the model, any system behavior to varying input data between certain limits;
- adaptability - a feature that requires taking into account the new information that may occur at a given moment;
- robustness - the results obtained by creating the model must be credible;
- totality - to reflect all the main problems of the system;
- easiness - the user-to-model dialogue to be easy to do.

The model, as an instrument of the scientific sphere, is used in various disciplines in different fields of activity. Depending on the method of constructing the models, of the nature of their elements, their particularities, there is a wide variety of models, and hence some difficulty in classifying them, and especially in identifying a particular type of model.

Thus, according to the nature of the component elements, models can be[2]:

- physical, whose components are of a physical nature (eg models, simulators, etc.);
- abstract, comprising abstract elements (variables, equations, functions);
- hybrid, having combinations of physical and abstract nature.

According to the representation of systems, real phenomena or processes, one can distinguish:

- analogical models that use some physical properties of a certain nature to represent other physical properties of a different nature;
- symbolic or mathematical models, in which the properties of the system are expressed by a set of parameters, and relations describing its functionality by logical or quantitative mathematical functions;
- iconic patterns that represent its image (maps, thumbnails, layouts, etc.) to other dimensions.

By the nature and degree of knowledge of the relations between the elements of the real system, models can be deterministic or probabilistic.

In the case of deterministic models, the causal relationship is a mutual correspondence, which can be described with sufficient accuracy, and the values taken by the output variables and the relationships between the defining parameters of the modeled system and the function defining their interaction are determined and known. As a result, the set input parameters correspond to the output parameters determined, whenever the process characteristic of the system is repeated.

In the case of probabilistic (stochastic) models, the knowledge of the system by its model has a probabilistic character, generated by the fact that the variables describing the system, the phenomenon or the modeling process have a random aspect with a known distribution.

3. The military model

The scientific substantiation of the decision requires carrying out a large volume of complex calculations using probabilistic mathematical methods (models) that take into account random factors in the conduct of combat actions. Models are useful tools that can be used by commander and staff to identify solutions to issues that arise in all stages of training and conduct of the operation. The multitude of information gathered is processed and disseminated, as the success of the operation rests with the one who holds

[2] *Ibidem*, p. 42.

information, the one who collects a full volume of information, processes it appropriately, makes scientifically substantiated decisions, formulates and delivers in time the missions of the subordinates.

3.1. Principles of mathematical modeling in the military system

The methodological framework for approaching the mathematical modeling of operation is based on a series of six principles[3] (see Figure no. 1).

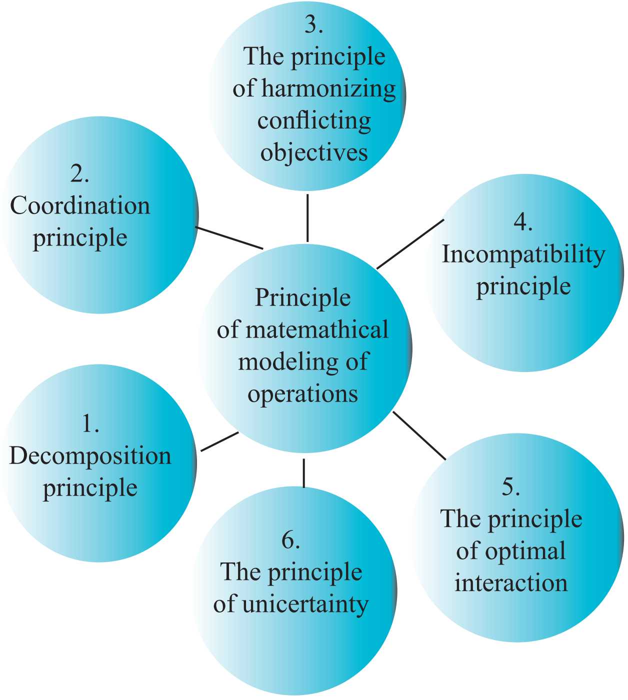

3.
The principle of harmonizing conflicting objectives
2.
Coordination principle
4.
Incompatibility principle
Principle of matemathical modeling of operations
1.
Decomposition principle
5.
The principle of optimal interaction
6.
The principle of unicertainty

Figure no. 1: Principles of mathematical modeling in the military system

Decomposition principle

This principle requires the analysis of a great problem of optimization by the study of local subproblems and their independent solving without taking into account the solutions of the other activities (global optimum). As a result of the introduction of artificial restrictions to the subproblems resulting from the decomposition, a suboptimal (satisfactory) solution can be obtained.

Coordination principle

This principle addresses the management of large systems composed of hierarchically and decentralized interconnected subsystems; it can be as effective as centralized management, provided there is a complex system. Even if it is possible, it is not advantageous due to the large number of feed-back loops of nonlinearity and other factors, including different units of measurement. On the other hand, decentralized (independent) management is not a solution, due to the inherent propensity of systems to disregard the requirements of other subsystems.

The principle of harmonizing the conflicting objectives, existing at subsystem level, in order to ensure the achievement of the global objectives. This principle generates a series of methods and techniques to approach the mathematical modeling of operation, meaning that the goal of a higher echelon becomes a control rule at subordinate echelon levels, decisions being taken at the hierarchical level, depending on the global situation and the system restrictions.

Incompatibility principle

This principle is characterized by the fact that when the complexity of the system is high, the possibility of analyzing the behavior of the system with a modeling tool is reduced to a certain level, thus the accuracy and relevance can be mutually exclusive.

The principle of optimal interaction

When a complex system composed of optimal systems is optimal, then each subsystem is considered optimal in interaction, and vice versa.

The principle of uncertainty

In a complex system consisting of several correlated subsystems, state i of the subsystem "i" and its correlation with the other subsystems can be determined simultaneously to a certain degree of precision.

The military-specific mathematical model generally means a formalized (analytical or logical) description of military action so as to adequately reflect the particularities of this action, take into account its main characteristics and allow results to be obtained with the imposed precision.

[3] Fang Deng, Lin Zhu, Jie Chen, "Application of cellular automata in military complex system", *31st Youth Academic Annual Conference of Chinese Association of Automation (YAC)*, Wuhan, 2016, pp. 281-285.

The mathematical models of military actions must contain requirements[4] that take into account the general principles of military tactics, strategy and art, as well as the combat composition of the tactical and operational device necessary to accomplish the mission. Models must be functional, providing permanent data to the commander. They are prepared in advance and should represent mathematical and logical analogies of a typical military action that takes into account specific elements in the military field, such as: the real organizational structure of the participating forces, their quantitative and qualitative organic composition, operational tactics provided in regulations, instructions and other normative acts. The authors of the study "Modeling earthquake activity using cellular automata" recommend that models should be developed that also take into account the geographical and military characteristics of the lines of action that are limited to a specific part of the military action.

3.2. The phases of developing a military model

The efficiency of modeling must be a feature of each design phase of the new system. At the same time, a number of operations are taking place as part of the system analysis.

In the following, we will present a step-by-step analysis of the different phases[5] of a mathematical model elaboration, staging closely related to other phases of the system analysis (see Figure no. 2).

Phase 1

The first stage includes actions that are preparatory in nature, having as main purpose knowing the realities of the military.

This phase consists of a series of stages.

System analysis

By using the purpose and destination of the model, it is possible to specify the main parameters that can be taken into account considering the initial data that will be the object of the military action. These parameters influence the general principles of military art, operational-tactical norms stipulated in regulations and instructions, as well as other elements characteristic to combat.

The mathematical model is developed by a multidisciplinary college consisting of staff analysts or military specialists in the field in which they simulate, mathematicians and programmers. The role of the staff analyst is to establish as accurately as possible the purpose of the model and to formulate the main tactical and operational requirements needed for the model to be developed.

In most frequent cases, one can track:

- simulation of combat under various conditions;
- leadership organisation at different echelons, in relation to one or more objective factors;
- the decomposition of the system into subsystems takes into account the criteria by which it can be done; they are physical or functional;
- explaining the limits of the military system;
- determining the variables of the military system − these, like all systems, have exogenous variables coming from the outside, with influences on the endogenous variables − variables determined by the components within the system.

Characteristic for this phase is the specificity of the informational-decision methodologies that require a more detailed description of the decisional processes focused mainly on the understanding of the decision-making by the commanders. As a result, the main elements of knowing the reality required for modeling are the description of the logic of the decisional processes and the objectives of the system.

Phase 2

The second phase consists in the actual design of the model. This operation is reflected in the use of a specific modeling tool, chosen from the wide variety of operational research available.

[4] G. Ioakeim Georgoudas, Georgios Sirakoulis, I. Andreadis, "Modelling earthquake activity features using cellular automata", *Math. Comput. Model*, 2007, vol. 46, pp. 124-137.

[5] Ion Stoian, *Elemente de programare liniară – aplicații în domeniul militar*, Editura Academiei Înalte Studii Militare, 2002, pp. 16-19.

The model is inseparable from the rational approach of the system management in both programmable and non-programmable processes. The development of mathematical models allows the following activities to be carried out:

1. The foundation and choice of the mathematical method of solving military problems by: analytical methods; stochastic (probabilistic) methods; mixed methods; the choice of the main mathematical dependencies (restrictions) on the basis of which the actions of combatants are assessed at each stage of the leadership or at each stage of the battle.
2. Determining the initial data needed to configure the model.
3. Deduction or identification of mathematical formulas for restrictions.
4. Choosing the probability characteristics that define: the effectiveness of system components in each phase; determining and normalizing restrictions and tolerances; the mathematical formulation of the problem; developing the list of input and output data from the system; identification of model parameters by direct or indirect method; elaboration of algorithms and calculation program.

Phase 3

The third phase – modeling – consists of comparing the obtained model with the reality. Relevant stages for this phase are: development of validation criteria and validation of the model; optimizing system behavior and implementing the model. As personalizing the decision is taken into account, there is checked the set of variables that refer to the manager and the contextual variables related to the social influences of the organizational context.

The data required for implementation must meet the following requirements: fairness; facility; high frequency of data collection and, at the same time, must reflect participatory managerial approaches. At this stage, the uncertainty and risk of decision inherent in the current conditions are minimized due to the high accuracy and completeness of the data set up in the model. The hindering factor in gaining greater precision is given by the complexity of the military systems being approached. If any information gathered would have perfect accuracy, we would work with variables and deterministic patterns, a situation rejected by real conditions.

Phase 4

The fourth phase consists in capitalizing on developed models and their use in practice. The advantages of mathematical modeling are underlined by the substantial reduction of the subjective character of the decision, and the valorisation of the models conceived with the modern decision-making tool increases the quality of the decision and ensures a competent solution of situations of great complexity. This phase of modeling reflects by enhancing the functionality and effectiveness of decision-making. Using the model in practice provides a picture of information with overriding decision-making functions and multidimensional decision making. Synthetically, the outcomes of past work are mirrored, which also form the basis of normative directions for future decision-making activities.

On the basis of the four phases of mathematical modeling, practically, we try to obtain optimal solutions or at least close to the optimal aspect, which is, in fact, the main objective of mathematical modeling.

Three methods can be used to achieve this goal:

- *Exact optimization procedures*, which actually involve obtaining the best solution in terms of a formulated criterion, which supposes that there are no better solutions. In this case, the error is null.
- *Heuristic methods* that lead to a satisfactory solution, good or even very good, which does not imply the certainty of optimality or the possibility to estimate the deviation from the optimal. For this reason, the error of models can not be kept under control.
- *Approximate methods*, which require obtaining a solution close to the optimum through successive iterations. In this case, the error can be controlled.

The main purpose of any model is to describe the internal structure, input and output elements

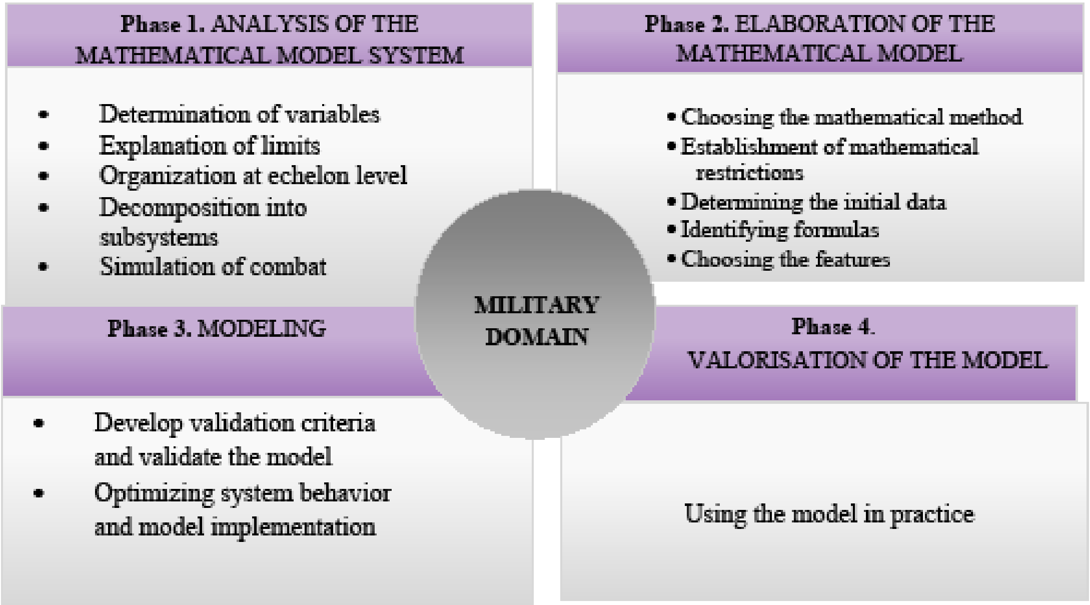

Phase 1. ANALYSIS OF THE MATHEMATICAL MODEL SYSTEM
Determination of variables
Explanation of limits
Organization at echelon level
Decomposition into subsystems
Simulation of combat
Phase 2. ELABORATION OF THE MATHEMATICAL MODEL
Choosing the mathematical method
Establishment of mathematical restrictions
Determining the initial data
Identifying formulas
Choosing the features
MILITARY DOMAIN
Phase 3. MODELING
Develop validation criteria and validate the model
Optimizing system behavior and model implementation
Phase 4. VALORISATION OF THE MODEL
Using the model in practice

Figure no. 2: The four phases of the military domain

(flows), relationships, types of linkages between constituents, restrictions imposed on model operation. The behavior of the model is evaluated by the state of the output variables, which is logically determined by the input variables and parameters, as well as the internal structure and the restrictions imposed for the functioning of the model. As a rule, dependence of output variables on input variables is determined by the logical structure of the adopted model.

Conclusions

Modeling is a method of researching systems, processes or phenomena by substituting the real object, based on the identification of physical or mathematical similarities between two systems in relation to certain established characteristics.

By a judicious structure, mathematical models specific to the military field allow to provide, directly and with sufficient precision, optimal solutions in planning and conducting military actions. Modeling and the model intertwine with each other at different stages of research, however they must not be limited to those existing at one time but must be studied and improved with other new methods that appear in other areas of science and which can offer interesting solutions to the studied problems.

It is essential that the choice of methods takes into account not only the mathematical aspect but, above all, the specificity of tactical and operational art, practice and warfare. These requirements can be met by using research methods specific to the theory of decisions.

It is essential that the choice of methods takes into account not only the mathematical aspect.

BIBLIOGRAPHY:

1. BRYDE, Daniel; BROQUETAS, Michael; VOLM, John M, “The project benefits of Building Information Modelling (BIM)”, *International Journal of Project Management*, 2013.

2. DENG, Fang; ZHU, Lin; CHEN, Jie “Application of cellular automata in military complex system”, *31st Youth Academic Annual Conference of Chinese Association of Automation (YAC)*, Wuhan, 2016.

3. GEORGOUDAS, Ioakeim G.; SIRAKOULIS, Georgios. C.; ANDREADIS, I. Th; “Modelling earthquake activity features using cellular automata”, *Mathematical and Computer Modelling*, vol. 46, 2007.

4. ILIE, Gheorghe; STOIAN, Ion; ALEXANDRESCU, Gelu, *Modelarea sistemelor şi proceselor*, Editura Universităţii Naţionale de Apărare “Carol I”, 2005.

5. STOIAN, Ion, *Elemente de programare liniară – aplicaţii în domeniul militar*, Editura Academiei de Înalte Studii Militare, 2002.

International Symposium “INTER-INSTITUTIONAL COOPERATION – A TOOL FOR ACHIEVING SECURITY AT NATIONAL AND INTERNATIONAL LEVELS”

25 May 2017

On May 25, 2017, the Centre for Defence and Security Strategic Studies organised the International Symposium on “Inter-institutional Cooperation – A Tool for Achieving Security at National and International Levels”. The event took place in the Senate Hall of “Carol I” National Defence University and was honoured by the presence of specialists from the Ministry of National Defence, the Ministry of Internal Affairs and the Ministry of Foreign Affairs, thus contributing to the consolidation of a solid and coherent inter-institutional cooperation.

Group photo with the participants at the Symposium

During the scientific activity, the need to develop and strengthen inter-institutional cooperation in the field of security and defence was highlighted in response to risks and threats to national and international security.

Photo: Aspect from the Scientific Symposium

At the event, moderated by Colonel Florian Cîrciumaru, PhD there were three scientific papers, as follows:

- "Cooperation within the National Emergency Situation Management System – a perspective of the Operational Centre for Special Emergency Situations, Ministry of Foreign Affairs", presented by Brigadier General (r) dr. Liviu-Mihai DĂNILĂ, Head of Operational Centre for Special Emergency Situations within the Ministry of Foreign Affairs,

- "International cooperation on armaments control and Confidence and Security Building Measures (CSBM). Recent Trends at the OSCE Level", delivered by Colonel Ovidiu FIZEȘAN, from the National Military Command Centre (Nucleus) and

- "Institutional Resilience Growth to Counter National Security Threats", presented by the Police Chief Commissioner Ștefan SĂVULESCU and the Police Commissioner Mihaela ŢONE from the Ministry of Internal Affairs.

Photo: Aspect from the Scientific Symposium

We believe that the event has achieved its objectives, namely: to facilitate an in-depth understanding of certain issues related to inter-institutional cooperation at national and international level; to help create a framework for guidance and exchange of views between specialists; to promote strategic and security culture, and to disseminate the results of professional expertise and the scientific research of practitioners and theorists in the field of security and defence.

Andra PÎNZARIU [*]

[*] Andra PÎNZARIU is working in the Scientific Events and Cooperation Department within Centre for Defence and Security Strategic Studies from "Carol I" National Defence University, Bucharest, Romania. E-mail: pinzariu.andrea@unap.ro

Activities of the Centre for Defence and Security Strategic Studies

APRIL - JUNE 2017

In the following, we are going to present the activities organised by the Centre for Defence and Security Strategic Studies (CDSSS) in the analysed period, as well as issued publications.

On May 25 2017, CDSSS organised, in the Senate Hall of "Carol I" National Defence University, the International Symposium on "*Interagency Cooperation as a Tool of National and International Security*". The activity was honoured by the presence of specialists from the Ministry of National Defence, the Ministry of Internal Affairs and the Ministry of Foreign Affairs, contributing thus to an enhanced and coherent interinstitutional cooperation.

Aspect from the Symposium of 25 May 2017

Strategic Colloquium, the monthly supplement of *Strategic Impact* quarterly, published in April (in Romanian language) an article titled *The W32. Stuxnet malware security implications*, elaborated by Robert Dragoş, who has completed a volunteer internship at CDSSS during April- June.

Those interested in publishing in *Strategic Colloquium* may submit proposals at the following e-mail addresses: catalina.todor@unap.ro or cssas@unap.ro.

The monthly public lectures held at the Palace of the National Military Circle during this period covered the following topics: in April, Ms. Cristina Bogzeanu, PhD. Researcher exposed on *Security and Defence in EU in the context of Brexit. Central Concepts and Recent Evolutions*, in May, Cristian Băhnăreanu PhD. Senior Researcher held a presentation on *Defence Expenditure in (Inter)National Security Equation*, and in June, Marius Potîrniche PhD. Researcher lectured on the *Terminology of war - clarification, confusion, utility*.

In the second part of 2017, CDSSS organises a Workshop on "*Military Sciences - Security Sciences - Conceptual Landmarks*", followed by the International Scientific Conference STRATEGIES XXI, with the theme "*The Complex and Dynamic Nature of the Security Environment*" on 07-08 December.

Details regarding scientific activities organised by CDSSS are announced on the website: http://cssas.unap.ro/en/events.htm

Raluca STAN[*]

[*] Raluca STAN is working in the Scientific Events and Cooperation Department within Centre for Defence and Security Strategic Studies from "Carol I" National Defence University, Bucharest, Romania. E-mail: stan.raluca@unap.ro

GUIDE FOR AUTHORS

We welcome those interested in publishing articles in the bilingual academic journal *Strategic Impact*, while subjecting their attention towards aspects to consider upon drafting their articles.

ARTICLE LENGTH may vary between a minimum of 6 pages and a maximum of 14 pages (including bibliography and notes, tables and figures, if any). Page settings: margins - 2 cm, A 4 format. The article shall be written in Times New Roman font, size 12, one line spacing. The document shall be saved as Word 2003 (.doc). The name of the document shall contain the author's name.

ARTICLE STRUCTURE

- Title (centred, capital, bold characters, font 24).
- A short presentation of the author, comprising the following elements: given name, last name (the latter shall be written in capital letters, to avoid confusion), main institutional affiliation and position held, military rank, academic title, scientific title (PhD. title or PhD. candidate – domain and university), city and country of residence, e-mail address.
- A relevant abstract, which is not to exceed 150 words (italic characters)
- 5-8 relevant key-words (italic characters)
- Introduction / preliminary considerations
- 2 - 4 chapters (subchapters if applicable)
- Conclusions.
- Tables / graphics / figures shall be sent in .jpeg / .png. / .tiff. format as well.

In the case of tables, please mention above "**Table no. X**: Title", while in the case of figures there shall be mentioned below (eg. maps etc.), "**Figure no. X:** Title" and the source, if applicable, shall be mentioned in a footnote.

REFERENCES shall be made according to academic regulations, in the form of ***footnotes***. All quoted works shall be mentioned in the references, as seen below.

Example of book: Joshua S. Goldstein; Jon C. Pevehouse, *International Relations*, Longman Publishinghouse, 2010, pp. 356-382.

Example of article: Gheorghe Calopăreanu, "Providing Security through Education and Training in the European Union" in *Strategic Impact* no. 2 /2013, Bucharest, "Carol I" National Defence University.

Electronic sources shall be indicated in full, at the same time mentioning what the source represents (in the case of endnotes, the following mention shall be made: accessed on month, day, year). *Example of article*: John N. Nielsen, "Strategic Shock in North Africa", in *Grand strategy: the View from Oregon*, available at http://geopolicraticus.wordpress.com/2011/03/03/strategic-shock-in-north-africa/, accessed on 10.03.2017.

BIBLIOGRAPHY shall contain all studied works, numbered, in alphabetical order, as seen below.

Example of book: GOLDSTEIN, Joshua S.; PEVEHOUSE, Jon C., *International Relations,* Longman Publishinghouse, 2010.

Example of article: CALOPĂREANU, Gheorghe, "Providing Security through Education and Training in the European Union" in *Strategic Impact* no. 2 /2013, Bucharest, "Carol I" National Defence University.

Electronic sources shall be indicated in full, at the same time mentioning what the source represents. *Example of article*: NIELSEN, John N., "Strategic Shock in North Africa", in *Grand strategy: the View from Oregon*, http://geopolicraticus.wordpress.com/2011/03/03/strategic-shock-in-north-africa/.

Nota Bene: Titles of works shall be mentioned in the language in which they were consulted, with transliteration in Latin alphabet if there is the case and, preferably, translation in English language of the titles.

SELECTION CRITERIA are the following:

- the theme of the article must be in line with the subjects dealt by the journal: up-to-date topics related to political-military aspects, security, defence, geopolitics and geostrategies, international relations, intelligence;
- the quality of the scientific content;
- originality of the paper;
- novelty character – it should not have been priorly published;
- a relevant bibliography comprising recent and prestigious specialized works, including books;
- the text must be written in good English (British or American usage is accepted, but not a mixture of these).
- adequacy to the editorial standards adopted by the journal.

SCIENTIFIC EVALUATION PROCESS is developed according to the principle *double blind peer review*, by university teaching staff and scientific researchers with expertise in the field of the article. The author's identity is not known by evaluators and the name of the evaluators is not made known to authors. Authors are informed of the conclusions of the evaluation report, which represent the argument for accepting/rejecting an article. Consequently to the evaluation, there are three possibilities: a) the article is accepted for publication as such or with minor changes; b) the article may be published if the author makes recommended improvements (of content or of linguistic nature); c) the article is rejected. Previous to scientific evaluation, articles are subject to an *antiplagiarism analysis*.

SUBMISSION:

Authors will send their articles in English to the editor's e-mail address, **impactstrategic@unap.ro**, preferably according to the following time schedule: 15 December (no. 1); 15 March (no. 2); 15 June (no. 3) and 15 September (no. 4). If the article is accepted for publication, an integral translation of the article for the Romanian edition of the journal will be provided by the editor.

NOTA BENE:

By submitting their materials for evaluation and publication, the authors acknowledge that they have not published their works so far and that they possess full copyrights for them.

Parts derived from other publications should have proper references.

Authors bear full responsibility for the content of their works and for non-disclosure of classified information – according to respective law regulations.

Editors reserve the right to request authors or to make any changes considered necessary. Authors give their consent to possible changes of their articles, resulting from review processes, language corrections and other actions regarding editing of materials. The authors also give their consent to possible shortening of articles in case they exceed permitted volume.

Authors are not required any fees for publication and are not retributed.

Authors are fully responsible for their articles' content, according to the provisions of *Law no. 206/2004 regarding good conduct in scientific research, technological development and innovation*.

Published articles are subject to the Copyright Law. All rights are reserved to "Carol I" National Defence University, irrespective if the whole material is taken into consideration or just a part of it, especially the rights regarding translation, re-printing, re-use of illustrations, quotes, dissemination by mass-media, reproduction on microfilms or in any other way and stocking in international data bases. Any reproduction is authorized without any afferent fee, provided that the source is mentioned.

Failing to comply with these rules shall trigger article's rejection. Sending an article to the editor implies the author's agreement on all aspects mentioned above.

For more details on our publication, you can access our site, http://cssas.unap.ro/en/periodicals.htm or contact the editors at impactstrategic@unap.ro.

“CAROL I” NATIONAL DEFENCE UNIVERSITY PUBLISHING HOUSE

Director: Colonel Alexandru STOICA, PhD Lecturer

The publication consists of 74 pages.

“Carol I” National Defence University Printing House
Șoseaua Panduri 68-72, Sector 5, Bucureşti
e-mail: editura@unap.ro
Tel: 004021/319.40.80/215

1635/2017

C. 88/2018