2 April June 2015

Romanian Military Thinking

Military Theory and Science Journal
Published by the Romanian Armed Forces General Staff

Founded in 1864 under the name "România Militară"
- English edition, 11th year -

Romanian Military Thinking

PUBLISHER
ROMANIAN ARMED FORCES GENERAL STAFF

EDITORIAL STAFF ADDRESS
110 Izvor Street, Sector 5, Bucharest
Postal code: 050564
Telephone: +4021.410.40.40/1001731; 1001732
Tel/Fax: +4021.319.56.63
http://www.smg.mapn.ro/gmr
***Romanian Military Thinking** Journal*
is issued in March, June, September, December.
ISSN 1841-4451 ~ Print
ISSN 1842-824X ~ Online

HIGH ROYAL DECREE NO. 3663 THROUGH WHICH "MILITARY ROMANIA" BECOMES THE OFFICIAL JOURNAL OF THE GENERAL STAFF

"Art. I. - The official journal named "Military Romania" is founded at the General Staff, starting 1 January 1898, in which all officers within the Armed Forces will find military studies, which interest their training.

Through the agency of this journal all officers, belonging to all branches, who are in service, will be able to publish their personal papers and the ones that interest the Armed Forces".

Carol - King of Romania
Issued in Bucureşti on 8 December 1897

Order *"Meritul Cultural"*
in the rank of *"Officer"*,
F Category – *"Promotion of Culture"*
(Presidential Decree no. 483 on 30.06.2014)

2 April June 2015

Romanian Military Thinking

Military Theory and Science Journal
Published by the Romanian Armed Forces General Staff

Founded in 1864 under the name "Military Romania"
- English edition, 11th year -

Romanian Military Thinking Journal Awards

These awards are yearly bestowed, by the Romanian Armed Forces General Staff, on the most valuable works in the field of military science, published in the previous year.

Award "Division General Ştefan Fălcoianu"

Award "Brigadier General Constantin Hîrjeu"

Award "Marshal Alexandru Averescu"

Award "Army Corps General Ioan Sichitiu"

Award "Lieutenant Colonel Mircea Tomescu"

Romanian Military Thinking is a scientific journal with acknowledged prestige in the field of *"Military Science, Intelligence and Public Order"*, in keeping with the evaluation carried out by the National Council for Titles, Diplomas and Certificates (CNATDCU) in 2011 (http://www.cnatdcu.ro/wp-content/uploads/2011/11/reviste-militare1.pdf)

Romanian Military Thinking Journal is included in the Journal Master List of the Index Copernicus International database and EBSCO's International Security & Counter-Terrorism Reference Center database

Authors assume full intellectual responsibility for the articles submitted to the editorial staff, in keeping with Law no. 206, 27.05.2004

Contents | Contenu

Editorial | Editorial

Contents		Contenu
Strategic Credibility Consolidation *Colonel Dr Mircea TĂNASE*	7	La consolidation de la crédibilité stratégique *Colonel dr. Mircea TĂNASE*

Military Science | Science militaire

Contents		Contenu
Financial Resource Management Specific to Contemporary Military Affairs *Brigadier General Dr Florin JIANU*	11	La gestion des ressources financières spécifiques aux affaires militaires contemporaines *Général de brigade dr. Florin JIANU*
Potential National Measures to Counter Hybrid Warfare *Colonel Dr Crăişor-Constantin IONIŢĂ*	17	Potentielles mesures nationales de contrecarrer la guerre hybride *Colonel dr. Crăişor-Constantin IONIŢĂ*

Geopolitics • Geostrategy International Security | Géopolitique • Géostratégie Sécurité internationale

Contents		Contenu
Elements of Hybrid Warfare in the Islamic State of Iraq and Levant Operations *Colonel Liviu IONIŢĂ* *Lieutenant Colonel BEng Iulian AANIŢEI*	28	Eléments de la guerre hybride dans les actions de l'Etat islamique en Iraq et au Levant *Colonel Liviu IONIŢĂ* *Lieutenant-colonel ing. Iulian AANIŢEI*

The Role of the European Union in Conflict Resolution in Ukraine *Dr Mihaiela BUŞE*	40	Le rôle de l'Union européenne dans la résolution du conflit en Ukraine *Dr. Mihaiela BUŞE*
Cross-Cutting Security Challenges in Romania's Vicinity *Dr Cristina BOGZEANU*	52	Des enjeux transversaux de sécurité dans la proximité de la Roumanie *Dr. Cristina BOGZEANU*
The Strategic Partnership between Romania and the USA – A Cornerstone in the Current Security Context *Daniela RĂPAN*	68	Le parteneriat stratégique entre Roumanie et les Etats-Unis – un repère important dans le contexte actuel de sécurité *Daniela RĂPAN*
Russia and the Pivot to Asia (II) *Silviu PETRE*	76	Russie et le pivot vers l'Asie (II) *Silviu PETRE*

Cyber Security | Sécurité cybérnetique

Cyberspace Semantics at NATO Level *Colonel Dr BEng Dan COLESNIUC* *Major Marian TURLEI*	83	La sémantique du cyberespace de l'OTAN *Colonel dr. ing. Dan COLESNIUC* *Commandant Marian TURLEI*
Cyberspace Cartography *BEng Alexandra DINULESCU* *BEng Gheorghe URSULEAN*	95	La cartographie du cyberespace *Ing. Alexandra DINULESCU* *Ing. Gheorghe URSULEAN*
Advanced Persistent Cyber Threats Addressed to Military CIS *Major BEng Georgiana GULIMAN* *Captain BEng Alin-Marian PUNCIOIU*	108	Cyber-menaces persistantes avancées contre SIC militaires *Commandant* *ing. Georgiana GULIMAN* *Capitain ing. Alin-Marian PUNCIOIU*

Opinions

Opinions

States Sanctions Policy
– A Form of Undeclared War
General (r.) Dr Mihail ORZEAŢĂ

119 La politique de sanctions entre Etats
– une forme de guerre non déclarée
Général (r.) dr. Mihail ORZEAŢĂ

The Romanian Mountain Troops
– Between Historical Necessity
and Present Milestones
Lieutenant Colonel Nicolae USZKAI

131 Chasseurs alpines
de l'Armée Roumaine
– entre nécessité historique et repères
du présent
Lieutenant-colonel Nicolae USZKAI

Terrorism – A Continually Actual
Scourge
Dr Anelis-Vanina ISTRĂTESCU

139 Le terrorisme – un fléau intemporel
Dr. Anelis-Vanina ISTRĂTESCU

Considerations on the Influence
Various Types of Learning
and Technology Exercise
over Modern Education Mechanisms
Major Dr Dragoş BĂRBIERU

159 Considérations sur l'influence
des différents types d'apprentissage
et de la technologie
sur les mécanismes
de l'éducation moderne
Commandant dr. Dragoş BĂRBIERU

Pages of Military History

Pages de l'histoire militaire

Staff Officers
Training Abroad (1878-1940)
Colonel (r.) Dr Petre OTU

171 La formation des officier d'état major
à l'étrangère (1878-1940)
Colonel (r.) dr. Petre OTU

International Connections | Connexions internationales

Enhancing Interoperability – The Foundation for Effective NATO Operations *Dr James DERLETH*	182	L'amélioration de l'interoperabilite – le fondement de l'efficacité des opérations de l'OTAN *Dr. James DERLETH*

NATO News | Nouvelles de l'OTAN

Statement by NATO Defence Ministers	191	Déclaration des ministres de la Défense des pays de l'OTAN

Strategic Credibility Consolidation

Having as a central theme **"A strong Romania in Europe and the world"**, *Romania's National Security Strategy* for the period 2015-2019, adopted by the Parliament, will be the guiding document that defines national security interests and goals and ensures the strategic framework for the unitary organisation and coordination of the activities relating to national defence and security.

By lucidly assessing the current security environment, identifying the main threats, risks and vulnerabilities to Romania's fundamental interests, and formulating the courses of action to be followed in order to ensure national security, *Romania's National Security Strategy* becomes the instrument that lies at the basis of national defence planning for the next five years. Strategies, doctrines, programmes and plans will be developed by the institutions with responsibilities in the field in order to meet the goals set in this programmatic document.

Built on values such as dignity, social cohesion and assertion of national identity, constitutional democracy and rule of law, state and territorial integrity, the *Strategy* aims to meet the needs and expectations of society. It is directed towards each and every citizen, society as a whole, and state institutions. Through an integrative and multidimensional approach, which combines and balances defence and a series of other dimensions – public order, intelligence, counterintelligence, security, diplomacy, economy, infrastructure, education –, the new *National Security Strategy* ensures, under the concept of *"wider national security"*, compliance with the European security principles developed in the *European Security Strategy* and the *European Union Internal Security Strategy*.

As far as defence is concerned, Romania has to focus the strategic efforts on the defence and security of its citizens, of the national territory, as well as on the support provided for its allies and partners, in compliance with its commitments under international treaties. As for the military, the courses of action mentioned in the *Strategy* are aimed at strengthening the national defence capability, including through the effective use of NATO existing mechanisms and through the enhancement of military cooperation within the national territory and the Black Sea region. The strategic partnership with the USA and the membership of NATO and the EU are reaffirmed as pillars of foreign security policy, taking into consideration that the transatlantic relationship solidity depends on maintaining the US commitment to Europe as well as on the way in which the European allies and partners will allocate resources to develop their own defence capabilities.

Defence and security are beyond the responsibility of a single state. However, none of the Alliance members should rely solely on the European partners or NATO support, needing to have and develop their own military and security forces. The economic development of a country generates the necessary resources to cope with threats, risks and vulnerabilities and, in this respect, our new *Strategy* stipulates the continuation of the process of transformation, modernisation and equipment of the Romanian Armed Forces, the annual allocation of at least 2% of GDP to the defence budget, for 10 years, beginning in 2017, being a prerequisite for meeting the required performance standards as well as for achieving interoperability with the armed forces of other NATO member states.

Strengthening Romania's strategic credibility, through continuity in commitments and predictability in actions, in a dynamic, complex and increasingly difficult to predict international security environment, requires having a more important role and national presence in civilian missions and in military operations, by participating in monitoring missions and crisis management operations in the areas of priority interest.

In a European security architecture increasingly threatened by crises and conflicts, most of them asymmetric and hybrid, Romania can become a strong and safe country, a credible country, and a source of reliability. Therefore, to effectively implement the *National Security Strategy*, the consensus and cohesion at national level and the joint effort of all responsible institutions are necessary because, as far as vital issues for the country are concerned, options should be directed towards dialogue and consensus of opinions.

Situated at the crossroads of great geopolitical interests, Romania needs to preserve strategic balance in this area where dissonant regional security complexes interact. As for the mechanism of collective defence in the Euro-Atlantic area, the convergent goals and courses of action set by the *National Security Strategy* are meant to ensure consistency and strategic coherence in meeting commitments.

Colonel Dr Mircea TĂNASE

English version by
Diana Cristiana LUPU

La consolidation de la crédibilité stratégique

Sous le slogan **„Une Roumanie forte en Europe et dans le monde“**, *la Stratégie nationale de défense de la Roumanie* pour les années 2015-2019, approuvée par le Parlement, sera le document-guide qui définisse les intérêts et les objectives nationales de sécurité et qui va fournir le cadre stratégique pour l'organisation et la coordination unitaire des activités relatives à la défense et la sécurité nationale.

Grâce à une évaluation lucide de l'environnement actuel de sécurité, par l'identification des menaces principales, des risques et vulnérabilités aux intérêts fondamentaux de la Roumanie et par la formulation des directions d'action pour assurer la sécurité nationale, c'est *la Stratégie nationale de défense du Pays* qui devienne l'instrument qui prend en charge la planification de défense au niveau national pour les cinq prochaines années. Le pas suivant sera l'élaboration des stratégies, des doctrines, des programmes et des plans d'activité par les institutions ayant des responsabilités dans la réalisation des objectives assumées en vertu du ce document programmatique.

Fondée sur des valeurs comme la dignité, la cohésion civique et l'affirmation de l'identité nationale, la démocratie constitutionnelle et la primauté du droit, l'intégrité de l'Etat et celle territoriale, *la Stratégie* vise à répondre aux besoins et attentes de la société et du chaque citoyen, mais aussi à la société, dans son ensemble, et aux institutions de l'Etat. Par une approche intégrative et multidimensionnelle, où la défense se combine et réalise réciproquement une équilibre avec un certain nombre d'autres dimensions – ordre publique, l'activité de l'intelligence, de contre-espionnage et de la sécurité, la diplomatie, l'économie, les infrastructures, l'éducation –, la nouvelle *Stratégie nationale de défense du Pays* offre, par le concept de *„sécurité nationale élargie“*, la convergence avec les principes européens de sécurité, développés dans *la Stratégie européenne de sécurité* et *la Stratégie de sécurité intérieure de l'Union européenne.*

En ce qui concerne la dimension de la défense, la Roumanie doit concentrer ses efforts stratégiques pour la défense et la sécurité de ses citoyens, du son territoire national, mais aussi pour soutenir les Etats alliés et partenaires, conformément avec les engagements pris en vertu des traités internationaux. Dans le domaine militaire, les directions d'action de *la Stratégie* visent la consolidation de la capacité nationale de défense, y compris par l'utilisation efficiente des mécanismes existants au sein de l'OTAN, en renforçant la coopération militaire, sur le territoire nationale et dans la région de la Mer Noire. Le parteneriat stratégique avec les Etats-Unis, notre appartenance à l'OTAN et à l'UE sont réaffirmés en tant que des piliers de la politique étrangère et de sécurité, mais il faut tenir compte que la solidité de la relation transatlantique dépend de maintenir l'engagement des Etats-Unis en Europe, ainsi que la façon dont les alliés et les partenaires européens alloueront des ressources à développer leurs capacités de défense.

La défense et la sécurité dépassent le cadre de responsabilité d'un seul Etat, mais aucun des membres de l'Alliance ne doit pas uniquement compter sur le support militaire des partenaires européens ou de l'OTAN; donc, il est besoin de développer et de posséder ses propres forces militaires et de sécurité. Le développement économique d'un pays crée les ressources nécessaires pour répondre à toutes les menaces, les risques et les vulnérabilités et, à cet égard, notre nouvelle *Stratégie* prévoit la poursuite du processus de la transformation, la modernisation et la logistique de l'Armée Roumaine, par l'allocation annuelle du minimum 2% du PNB pour le budget de la défense, depuis 10 ans, au début de l'année 2017, comme une condition essentielle à la réalisation des normes de performance nécessaires, mais aussi pour assurer l'interopérabilité avec les armées d'autres Etats membres de l'Alliance.

La consolidation de la crédibilité stratégique de la Roumanie, par la continuité des engagements et la prévisibilité en actions, dans un environnement dynamique de la sécurité internationale, complexe et de plus en plus difficile à prévoir, il exige, plus loin, un accent approfondi sur le rôle et la présence nationale dans les missions civiles et dans les opérations militaires, de surveillance et de gestion des crises dans les domaines d'intérêts prioritaires.

Dans une architecture de sécurité européenne de plus en plus menacée par des crises et des conflits, les plus asymétriques et hybrides, c'est la Roumanie qui peut devenir un pays sûr et fort, une ressource crédible. Il est nécessaire, pour mettre en œuvre efficacement *la Stratégie nationale de défense du Pays*, de cohésion et de consensus au niveau national, de l'effort conjoint des institutions responsables, parce que, dans les questions vitales pour le pays, les choix doivent se diriger, par le dialogue, à l'identité des vues.

Située à l'intersection de routes de grand intérêt géopolitique, la Roumanie a l'obligation de maintenir un équilibre stratégique dans ce domaine d'interférence des complexes discordants de sécurité régionale. Dans le mécanisme de la responsabilité collective à défendre l'espace euro-atlantique, la convergence des objectives et directions d'action établies par *la Stratégie nationale de défense* visent à assurer la conséquence et la cohérence stratégique pour achever nos engagements.

Version française par
Alina PAPOI

FINANCIAL RESOURCE MANAGEMENT SPECIFIC TO CONTEMPORARY MILITARY AFFAIRS

Brigadier General Dr Florin JIANU

The article is aimed at analysing the theoretical foundations for engaging financial resources in designing and developing contemporary military affairs. According to American experts, this fundamental action focuses on three areas namely technology, organisation and doctrine, being supported by a country/organisation economic and financial power as well as its research and development sector. The above-mentioned domains interact, as military organisations have to adapt to be able to handle the changes in technology and geopolitical environment. In this context, the military activity, which is characterised by dynamism, complexity and interdependence, increasingly relies on strategic management.

Keywords*: military organisation transformation; financial resource management; government budget; military affairs*

Introduction

The transformations the Romanian military environment has undergone during the past years show that *"it is necessary to use material, financial, human resources and, last but not least, political resources and the civil society support as effectively as possible"*[1]. Transformation, as a result of the revolution in military affairs, involves the implementation of specific military technologies and the armed forces restructuring to meet the requirements proper to the information age. Therefore, combat units should be numerically smaller, interoperable, with high degree of independence and strike power, and the chain of command should be flexible, focusing on the ability to conduct network operations.

The changes occurred in the global political and military environment in the last two decades have resulted in significant developments in security

Brigadier General Dr Florin Jianu – Chief of the Financial Accounting Directorate, the Ministry of National Defence.

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

[1] *Planul strategic al M.Ap.N. 2010-2013*, p. 3, see www.mapn.ro/despre_mapn/informatii_generale/documente/plan_2009.pdf

and defence doctrines and strategies. It is clear to most military specialists in the field of military affairs that that these changes have led to new conceptual ways of addressing conflicts and crises involving military forces.

Thus, at the beginning of the third millennium, the rapid transformation of the battle space, in conjunction with the military applicability of new techniques and technologies, has managed to produce changes in the way the sources and resources for the design and conduct of military affairs are employed. The impossibility to precisely assess a potential aggressor sources and resources as well as the way it may use/access certain military techniques and technologies is a reason to analyse the design and conduct of contemporary military affairs.

Financial Resource Management

Our country's economy is currently affected by the ongoing global economic and financial crisis. Moreover, the effects of transition from centralised to market economy are still present. Economic and social realities have shown that in the era of business globalisation and regionalisation, of information technology, of reduced product and service life cycles, of increased labour productivity and technological efficiency, it cannot be conceived by any organisation to develop its activities in a turbulent, unsafe, risky or uncertain, sometimes chaotic environment, without taking special measures such as forecast, foresight, prospective analysis. In this respect, the military activity, which is characterised by dynamism, complexity, interdependence and novelty, increasingly relies on strategic management to respond optimally, effectively, efficiently, creatively and flexibly to the received social command. Actually, strategic management, as a management tool to implement the strategy, can be employed only if there is a clear vision of the organisation mission as well as of the activities that are necessary to achieve the set goals.

Financial and accounting management can be defined *as a function whose goals are: to permanently provide the economic entity with the necessary funds, to register and record the value of material and financial resources, and to control the efficiency of the operations that involve these funds*[2].

To achieve these goals, under the market economy conditions, it is necessary to ensure financial autonomy, which entails ensuring, based on economic criteria, the process of procuring funds, and putting on new bases the economic entity relationships with the external environment.

[2] *Management financiar-contabil*, see http://www.portal-contabilitate.ro/contabilitate-bucuresti/diverse-probleme-contabile/management-financiar-contabil/

The introduction of computers and information technology has provided financial and accounting management with the adequate tools for obtaining timely and complete information, which has resulted in a real support for the financial decision-making process and opportunities to optimise it.

Under the current conditions, accounting and financial management actions are aimed at dealing with risk and inflation, issues that have profound effects on all economic agents' decisions.

The changes our country has undergone in the process of transition to a functional market economy require important developments in the design and performance of financial accounting management, providing financial approaches with predictability, reconsidering financial methods and techniques taking into account the economic levers liberalisation, deepening economic analyses, accelerating the rotation of working capital, increasing the rigours of all activities mirroring in accounting, generalising the use of computers in all accounting activities, amplifying the preventive aspect of financial control, and focusing control over the financial aspects that are essential for the proper performance of activities.

All these aspects are meant to substantially improve the financial and accounting decision-making process, thereby achieving high efficiency in the use of economic entities resources.

Regardless of the political colour, any government tends to diversify the military structures financial resources and to use new criteria for their allocation based on quality, effectiveness and efficiency. To that end, funding sources are analysed at the level of each military institution thus addressing the issues related to financial resource management and financial autonomy of certain institutions. Without a rational design of military budgets and funding sources it cannot be ensured the functioning of military structures in the security and defence field under the current international security environment conditions. Since the planning period for NATO earmarked forces has expanded from 6 to 8-10 years there are necessary financial estimates that are not included in the Defence Planning Directive.

Usually, the Ministry of National Defence can finance activities and actions using funds from the following main sources: (1) the state budget; (2) external sources (external loans and funds received from military alliances or international organisations, e.g. the UN, NATO, for the participation in various military actions under the aegis of those organisations); (3) own revenues.

Since defence and security services meet collective needs, on behalf of the state, the necessary financial resources are mainly allocated by the state budget.

Thus financing from the budget is a basic condition to meet the national and international security commitments made by Romania. Using resources from the state budget is based on the destination principle approved by the budget law, so funding should cover both current and capital expenditures, in other words, operation financing and development financing.

"Military organisation, as an independent entity, undergoes continuous transformation, permanently interacting with the environment in which it operates, and the lever that streamlines this interaction is logistic management, which is achieved by the logistic decision-making process"[3].

Given the resources the Romanian state can allocate to defence and the trends to improve advanced military technology, the Armed Forces should develop, through own effort and international cooperation, the capabilities that are necessary so that they can be as close as possible, in terms of equipment and operability, to the armed forces of the states in the area of strategic interest for Romania.

To meet the requirements relating to restructuring and equipping the armed forces, it has been necessary a real increase in funding from about 710 million USD in 2000 to 1,190 million USD in 2007 and 1.5 billion EUR in 2014.

The national budget reflects the government's concept of the socio-economic situation of the nation, namely its social and economic priorities, and represents a statement on the government fiscal, financial and economic aims. The budget is, therefore, an important indicator of the government's intentions and a document of crucial importance in ensuring transparency and accountability as well as good governance. The budget approval by Parliament, before the government can spend money or collect revenues, results in increasing the ministerial accountability before Parliament and its committees.

Budgets are usually structured based on spending on sectors (education, health, public order and national security, defence) and organisations (ministries).

To optimise the use of resources the standards in force should be considered so that funds can be allocated based on unit costs (unit cost is the average cost per the unit of product or service or per the recipient of expenditure).

Given the multitude of needs that should be met with limited resources, users have to pay more attention to selecting the best methods of forecasting costs and to taking some measures to efficiently allocate and use financial resources. In order to properly evaluate both budget revenue and expenditure, different classical or modern methods have been employed, in an attempt to optimise the use of budgetary

[3] Colonel Dr Gheorghe Minculete, *Abordări ale managementului logistic în condiţii de transformare şi progres*, in *Gândirea militară românească*, no. 1, 2014, p. 48.

resources and link the expenditure of all institutions that contribute to achieving a particular goal.

Therefore, we conclude that if a country cannot bear the costs of achieving a strategic goal, it is forced to revise its goals to match the budget that it can bear; otherwise, an imbalance between goals and planned forces and between the defence budget and the programmes that must be supported occurs.

All the above-mentioned aspects considered, it follows that national security cannot be measured in money (financial resources), since we cannot appreciate something that has no price, which is invaluable, but in order to avoid serious errors money should be taken into account as political-military decisions are expressed, like it or not, in budgetary decisions.

For our country, an example of a lack of correlation between goals and budgetary programmes is the initial assumption of commitments to participating in international peacekeeping forces for an unspecified period of time, followed by the attempt to change the goals. The decision was taken after the pressure on the defence budget was too high (higher than initially estimated) and after practice and reality showed that some of the tasks undertaken, internally and externally, were affected because of non-financing. The conclusion is that the decisions were not scientifically substantiated and that, in the future, it is required the use of decision optimisation methods, so that changing the initial goals, even if justified, can be no longer necessary, as it generates effects in international relations relating to the seriousness and trust that should exist between partners.

Conclusions

The Romanian Armed Forces have undergone deep conceptual, structural and functional transformations, becoming a pioneer in the implementation of certain management methods that have been novel (not necessarily modern) for the public institutions in our country, in its desideratum to fully integrate into the Alliance structures.

Full integration into the Alliance requires, in addition to structural adjustment and achieving interoperability, the management elements procedural and methodological integration.

Employing sources and resources in the design and conduct of contemporary military affairs requires a constant adaptation to the changes in the security environment and a new philosophy regarding the approach to military affairs.

Under the concrete conditions related to contemporary developments, when international security is increasingly considered by societies, military affairs managers face a wide range of risks, threats and dangers, some of them particularly serious, such as terrorism and organised crime. All these risks, threats and dangers are dynamic, having diverse physiognomies and being addressed differently, which means that they have to be known, discovered, identified, decoded and monitored so that appropriate response strategies, methods and procedures can be developed.

The ability to allocate resources is considered by many experts the management power basis, because this activity involves the allocation of money, time, equipment, workforce and space. The role of managers is to make decisions about the use of time, to authorise actions, to establish programmes for the allocation and use of resources. Without the right to allocate resources, the manager's ability to fulfil his/her roles is substantially reduced[4].

In conclusion, we consider that the sources and resources management in the design and conduct of contemporary military affairs should first consider the managerial mechanism of ensuring the financial resources to really and continually support such affairs typology.

BIBLIOGRAPHY

1. Valentin-Stelian Bădescu, Cosmin Iordache, *Scurte consideraţii despre etica afacerilor militare contemporane*, in *Buletinul Universităţii Naţionale de Apărare "Carol I"*, no. 2, Editura Universităţii Naţionale de Apărare *"Carol I"*, Bucureşti, 2014.

2. Gabriel Gabor, *Paradigme în noile afaceri militare*, Editura T, Bucureşti, 2012.

3. Gabriel Gabor, Doina Mureşan, *Revoluţia în afacerile militare – un nou mod de ducere a războiului*, in *Buletinul Universităţii Naţionale de Apărare "Carol I"*, no. 3, Editura Universităţii Naţionale de Apărare *"Carol I"*, Bucureşti, 2013.

4. Ionel Hornea, *Revoluţia informaţională, baza revoluţiei în afaceri militare (RAM I)*, in *Buletin de teorie militară editat de Statul Major al Forţelor Terestre*, Year II, no. 3 (7), Bucureşti, 2010.

[4] Cornel Cucu, *Informaţii şi securitate militare, prezent şi perspectivă*, Editura CTEA, Bucureşti, 2009, p. 182.

POTENTIAL NATIONAL MEASURES TO COUNTER HYBRID WARFARE

Colonel Dr Crăişor-Constantin IONIŢĂ

The Ukraine Crisis represents, for many military theorists, a huge opportunity to restart debates regarding hybridity in future warfare. Some definitions and conceptual elements regarding hybrid threats and hybrid challenges have been developed since the Second Lebanon War of 2006 and improved after the Chechen War of 2008.

In this context, the author shows that, in conjunction with reviewing and adjusting strategies and warfighting concepts, the defence community should revaluate the force structure needed for future conflicts and build adequate capabilities. Given the wide range of threats that may require the need to employ various capabilities simultaneously, NATO and member states must continue to strive for greater joint operations and interdependence.

***Keywords**: hybrid warfare; hybrid threats; hybrid conflict; hybrid challenges; comprehensive approach*

The first decades of the new millennium have been marked by profound changes in the international security environment, with major implications in all areas of social life. The most important ones refer to the emergence of new crisis situations and strategic political-economic insecurity in the proximity of Romania and its allies, including the revival of the geostrategy of centres of influence and vital space worldwide.

Increasingly extremist political, religious and ethnic ideologies also amplify this insecure situation at global and regional levels while the absence of effective governance in many parts of the world creates sanctuaries for terrorists, criminals and insurgents. New emerging countries claiming monopoly of regional power centres and numerous states located in many regions of the world are unable or unwilling to exercise control over their territory or borders, leaving them open to exploitation by non-state actors. Weak or failed states, having stagnant economies, corrupt political institutions, environmental problems,

Colonel Dr Crăişor-Constantin Ioniţă – Strategic Planning Directorate, the General Staff, the Ministry of National Defence.

weak public health systems or epidemics, or those that are engaged in the multinational competition for natural resources often become conflict zones.

The new perception of citizens regarding the concept of *own and collective security* will probably change the current international security architecture and the geopolitical context in which states and non-state actors aim to achieve military and political objectives. The relationship between *security* and *defence* concepts is determined, more obviously, by the public perception of how the existential normality is affected as well as by its awareness of existing means and actions for protection and defence.

There is also an increasing tendency to replace territorial expansion with the interest and desire to influence events in a particular region or even globally, by giving up the idea of physical presence in an area of strategic interest for the need to control an area, by influencing it and possibly intervening, if necessary. Therefore, it is desirable to avoid direct armed confrontation and to change the will to produce substantial losses to an opponent.

The future security environment includes a combination of military and non-military challenges from state and non-state actors, with *hybrid warfare* as a new type of violent conflict being placed at the border of civil-military confrontations. A special feature of the actors involved in this new type of conflict is the willingness to minimally respect the international laws and to justify their *"Jus bellum"* actions.

Most likely, future conflicts will take place in urban areas, between people, among people, limiting the conventional military power efficient application. This issue will be exacerbated by the increased number of hostile states being equipped with weapons of mass destruction and sophisticated anti-access capabilities that can precede direct military options.

We consider that, by applying this new theory of hybrid war, it will cause realignments and chain reactions, at national, regional and global level, because it covers the whole spectrum of threats – from the completely symmetrical to asymmetrical ones –, comprises the full range of possible actors, from states to non-state actors and transnational ethnic groups as well as the whole spectrum of forms of combat – from the traditional to unconventional ones, including the struggle for getting a correct perception of the conflict development and popular support.

The major changes the conflicts' physiognomy has undergone demonstrate that the difficult task of maintaining national security is far beyond the capability and responsibility of a single country, and even the North Atlantic Alliance involvement. Moreover, security cannot be ensured by strictly using military power only but requires a different conceptual approach *(Comprehensive Approach – CA)* and a new intensity in waging civil-military actions, employing unconventional methods, indirect techniques and means to achieve strategic objectives. It will also require a systemic approach to the opponent *(PMESII*[1]*)* to meet the engagement requirements in multi-dimensional environments, such as energy, space or virtual ones.

As a result, it appears the necessity of flexible and agile structures and mechanisms, primarily in terms of tactics, to adapt rapidly to decision-making cycle (which is very short), the use of flexible and deployable structures, able to operate in urban crowded areas and to counter multiple methods of action, including terrorism, criminality and even portable conventional or mass destruction weapons.

After the Second World War, violent conflicts have been characterised by a more or less traditional approach, where asymmetric aspects have been especially used in intra-state conflicts *(figure 1)*.

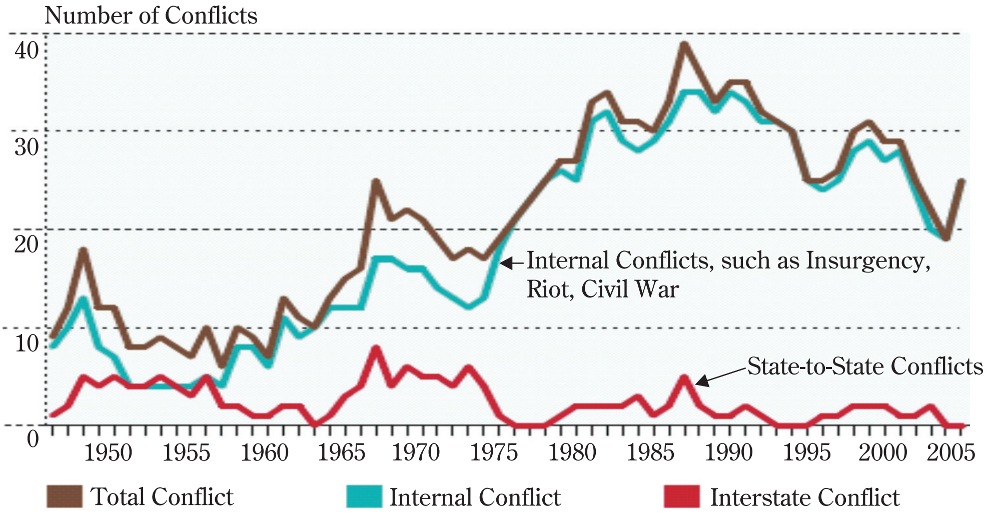


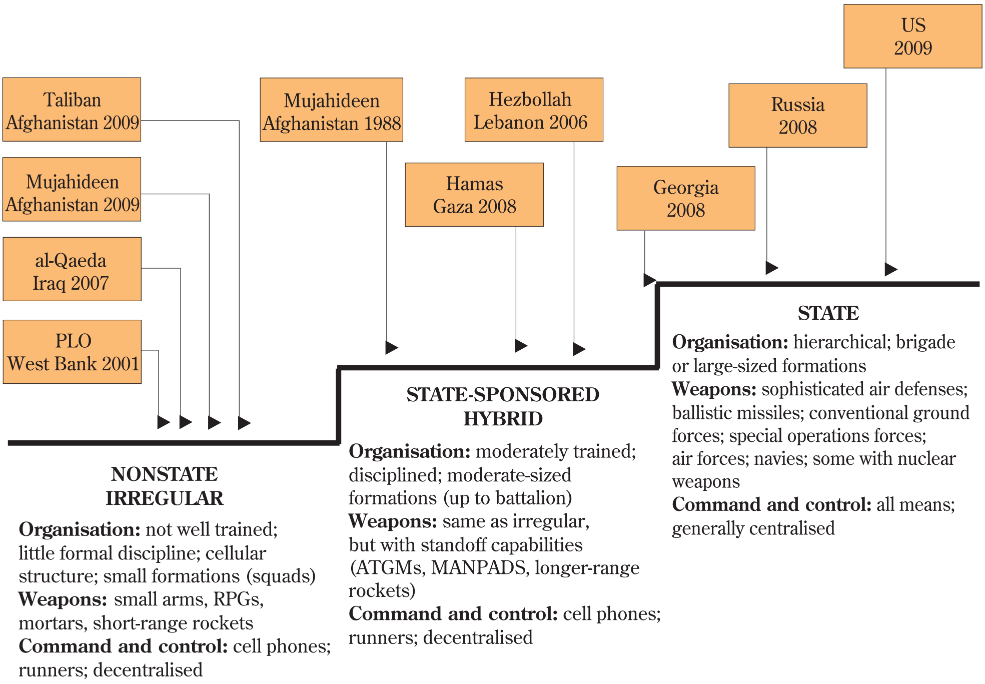
Figure 1: What is conventional in the conflicts in the period 1946 – 2005?[2]

We can notice, after 2005, a swift change in the physiognomy of conflicts, particularly after al-Qaeda became an international terrorist organisation and the first theory of *hybrid threats* appeared, nominating Iraqi insurgents, fanatical and religious factions in the Middle East – like Hezbollah and Hamas –, and foreign jihad's fighters in Afghanistan. Later, using the lessons learned in Afghanistan

[1] Political, Military, Economic, Social, Infrastructure, Information.

[2] J. Joseph Hewitt, Jonathan Wilkenfeld, Ted Robert Gurr, *Peace and Conflict 2008 Executive Summary*, Center for International Development and Conflict Management, University of Maryland.

and Iraq and the analyses carried out after the Second Lebanon War in 2006 and the Chechen War in 2008, US military theorists have added failing states and some hybrid groups in defining new hybrid threats. The evolution of this definition is shown in *figure 2*.



NONSTATE IRREGULAR

Organisation: not well trained; little formal discipline; cellular structure; small formations (squads)
Weapons: small arms, RPGs, mortars, short-range rockets
Command and control: cell phones; runners; decentralised

STATE-SPONSORED HYBRID

Organisation: moderately trained; disciplined; moderate-sized formations (up to battalion)
Weapons: same as irregular, but with standoff capabilities (ATGMs, MANPADS, longer-range rockets)
Command and control: cell phones; runners; decentralised

STATE

Organisation: hierarchical; brigade or large-sized formations
Weapons: sophisticated air defenses; ballistic missiles; conventional ground forces; special operations forces; air forces; navies; some with nuclear weapons
Command and control: all means; generally centralised

Figure 2: The Hybrid Threat Theory's Evolution[3]

At that time, the hybrid threat was more analysed as an issue than as a conceptual approach that requires settlement. Therefore, some military theorists have considered the conflicts in Iraq and Afghanistan as events that have accelerated the learning cycle for insurgents and terrorists (hybrid threats) in respect of the acquisition and use of increasingly effective fighting tactics and techniques as well as the continuous adaptation of *improvised explosive devices (IEDs)* to the operational environment.

The first NATO attempt to define this new threat was made by the *Supreme Allied Command Transformation (HQ SACT)* in 2009, when it described the hybrid threat as *"one perceived from any established or potential adversary, be it the states or non-state actors and terrorists, which has the ability, proven or probable, to use*

[3] David Johnson, *RAND OP295-1*, 2009.

simultaneously and in an adaptable way conventional and unconventional means to meet the set objective"[4]. NATO's concerns in the field were stopped in 2013.

Other definitions emerged in the 2009-2013 period to cover both hybrid threats and conflicts, being developed by the US, Canada or the UK. These definitions have been extensively presented in the article *"Este războiul hybrid ceva nou?" (Is Hybrid War Something New?)* in *Impact Strategic* Journal no. 4/2014.

What all these definitions have in common can be grouped into two main areas – **diverse actors** and **multiple military and non-military methods and techniques** that can be synergistically and innovatively employed by them. Actors can be state and/or non-state ones, including terrorists and organised crime. Military and non-military actions combine conventional forces and capabilities with unconventional tactics and formations, terrorist acts including violence and generalised coercion, public order destabilisation and cyber attacks. A list of such actions is provided in *table 1*:

Table 1

- Murder
- Genocide
- Intimidation
- Propaganda
- STRATCOM
- INFOOPS
- Arms Smuggling
- WMD
- Kidnapping
- Black Market
- Ethnic Cleansing
- Guerrilla Warfare
- Subversion
- Sabotage
- PSYOPS
- Illegal Funding
- Cyber War-Internet
- Starvation
- Asymmetric Warfare
- Extremist Indoctrination
- Attacks on Embassies
- Terrorism
- Rebellion
- Insurgency
- Suicide Bombing
- Piracy
- Drug Trafficking
- Governmental Corruption
- Transnational Crime
- Organised Crime

Hybrid wars mix the lethality of state conflicts with the fanaticism and duration of unconventional warfare. In such conflicts, future opponents (states, state-sponsored groups, or self-funded actors) could have access to modern military capabilities, such as encrypted control systems, portable systems, ground-to-air and ground-to-ground missiles and other modern lethal systems, seeking to promote prolonged insurgency, which employs unconventional actions such as ambushes, improvised explosive devices attacks and coercive killings. This kind of war could include countries that combine a variety of high-tech capabilities, like anti-satellite and anti-aircraft weapons, to conduct terrorist actions, information and cyber war against international financial targets. The destabilisation,

[4] *Multiple Future Projects. Navigating towards 2030. Findings and Recommendations*, April 2009, see www.act.nato.int/nato-multiple-futures-project-documents, p. 8

"decapitation" of administrations or the use of mass-media to influence are not new tactics but they have strategic effects.

Hybrid challenges are not limited to state or non-state actors. This is demonstrated by the fact that the repercussions of the Ukrainian Crisis may go beyond its borders. These challenges may include regional or even international actors that may lose their neutrality or impartiality. V. Putin's repeated assertion that *"ethnic Russians, wherever they live, are to be protected, not by the laws or constitutions of the countries in which they live, but by an external force, i.e., Russia"*[5] is incompatible with the international law architecture. This statement has forced organisations such as OSCE, NATO and the EU to take appropriate measures to penalise or diminish the threat to the member states. *Figure 3* shows the new aspects of hybrid war in conjunction with traditional confrontations.

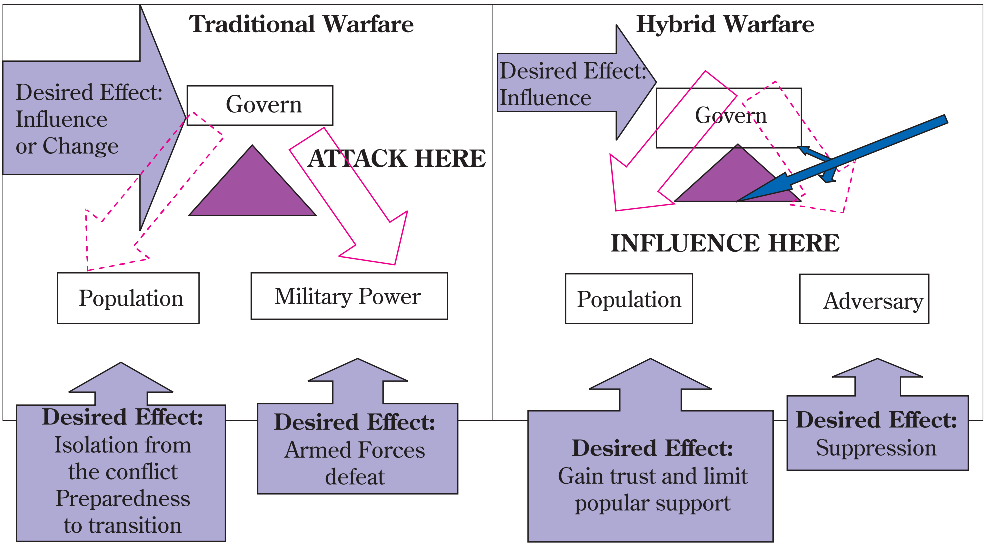
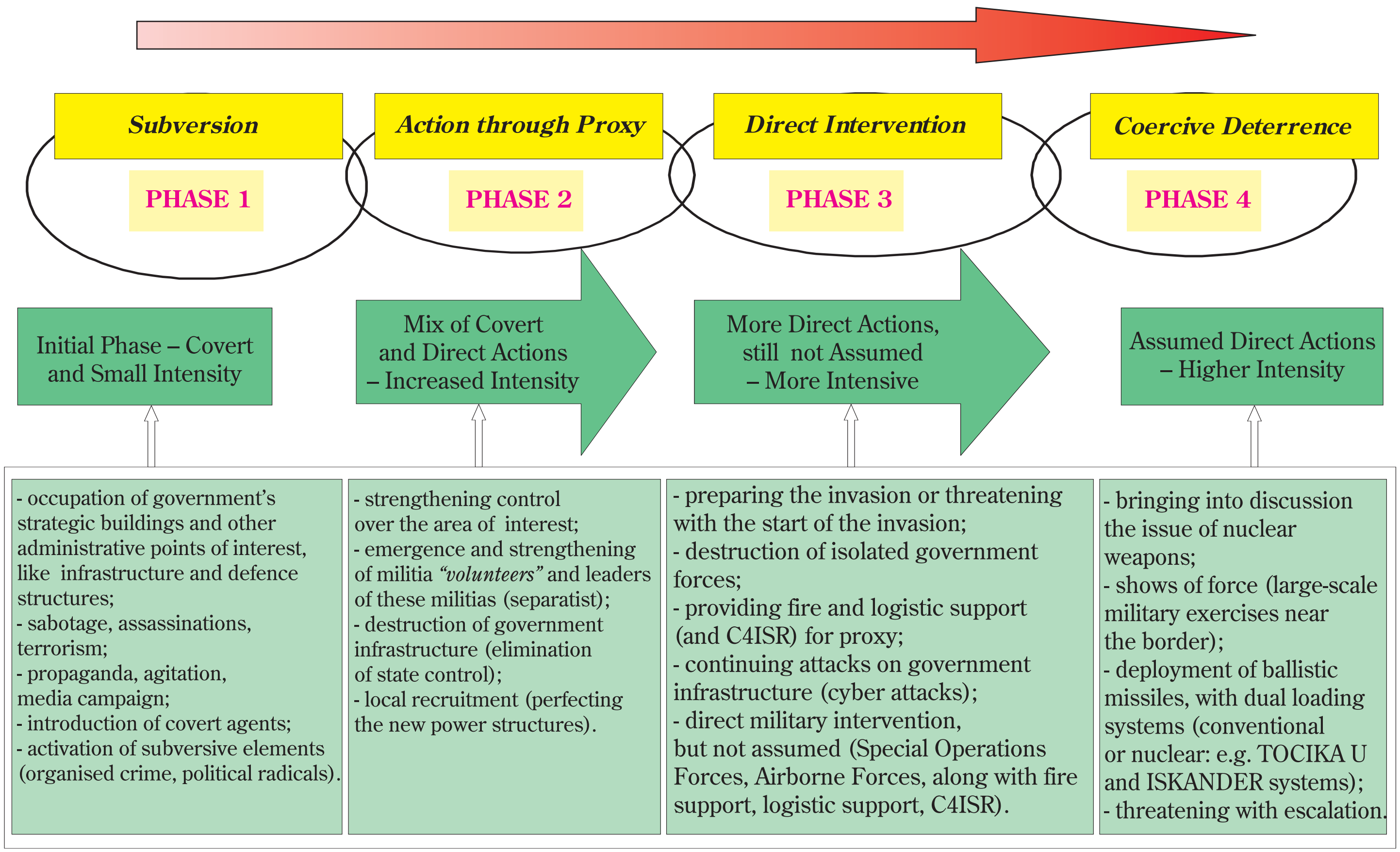

Traditional Warfare
Desired Effect: Influence or Change
Govern
ATTACK HERE
Population
Military Power
Desired Effect: Isolation from the conflict Preparedness to transition
Desired Effect: Armed Forces defeat
Hybrid Warfare
Desired Effect: Influence
Govern
INFLUENCE HERE
Population
Adversary
Desired Effect: Gain trust and limit popular support
Desired Effect: Suppression

Figure 3: Traditional warfare versus hybrid warfare

Hybrid wars are more than just confrontations between states and other armed groups. They implement various forms of conflict that highlight hybrid threats or conflicts at the maximum level possible. This is especially true due to the fact that hybrid wars can be carried out jointly by states and a variety of non-state actors, also involving many international security organisations.

The hybrid warfare has **four main phases**, which can be delimited by the degree of intensity and assuming of responsibility. In essence, as it can be seen in *figure 4*, it is about generating social chaos and its orientation to achieve the ultimate political objective.

[5] *Hybrid War, Hybrid Response?* – video on www.nato.int site, retrieved on 30 April 2015.



Subversion

PHASE 1

Action through Proxy

PHASE 2

Direct Intervention

PHASE 3

Coercive Deterrence

PHASE 4

Initial Phase – Covert and Small Intensity

Mix of Covert and Direct Actions – Increased Intensity

More Direct Actions, still not Assumed – More Intensive

Assumed Direct Actions – Higher Intensity

- occupation of government's strategic buildings and other administrative points of interest, like infrastructure and defence structures;
- sabotage, assassinations, terrorism;
- propaganda, agitation, media campaign;
- introduction of covert agents;
- activation of subversive elements (organised crime, political radicals).

- strengthening control over the area of interest;
- emergence and strengthening of militia *"volunteers"* and leaders of these militias (separatist);
- destruction of government infrastructure (elimination of state control);
- local recruitment (perfecting the new power structures).

- preparing the invasion or threatening with the start of the invasion;
- destruction of isolated government forces;
- providing fire and logistic support (and C4ISR) for proxy;
- continuing attacks on government infrastructure (cyber attacks);
- direct military intervention, but not assumed (Special Operations Forces, Airborne Forces, along with fire support, logistic support, C4ISR).

- bringing into discussion the issue of nuclear weapons;
- shows of force (large-scale military exercises near the border);
- deployment of ballistic missiles, with dual loading systems (conventional or nuclear: e.g. TOCIKA U and ISKANDER systems);
- threatening with escalation.

Figure 4: Hybrid War Phases

The first phase is to carry out **subversive activities**, being the initial phase characterised by lower intensity and covert actions, not officially assumed by any participant actor. Military and non-military actions are:

- occupation of government's strategic buildings and other administrative points of interest, like infrastructure and defence structures;
- sabotage, assassinations, terrorism;
- propaganda, agitation, media campaign;
- introduction of covert agents;
- activation of subversive elements (organised crime, political radicals).

The second phase is that of actions undertaken through **proxy/intermediaries**, being characterised by an increased intensity and a mix of covert and direct actions, such as:

- strengthening of control over the area of interest;
- emergence and strengthening of militia *"volunteers"* and leaders (separatist);
- destruction of government infrastructure (elimination of state control);
- local recruitment (perfecting the new power structures).

The third phase is the **direct intervention**, when the conflict increases in intensity and actions become more and more direct, but still not assumed. Among these actions, we can distinguish:

- preparing the invasion or threatening with the start of the invasion;
- destructing isolated government forces;
- providing fire and logistic support (and C4ISR) for proxy;
- continuing attacks on government infrastructure (cyber attacks);
- direct military intervention, but not assumed (Special Operations Forces, Airborne Forces, along with fire support, logistics support, C4ISR).

The fourth phase is to **coercively deter**, when the intensity is high, and actions are direct and assumed. The phase includes:

- bringing into discussion the issue of nuclear weapons;
- show of force (large-scale military exercises near the border);
- deploying ballistic missiles, with dual loading systems (conventional or nuclear: e.g. *TOCIKA U* and *ISKANDER* systems);
- threatening with escalation.

Hybrid war brings the danger of erasing the boundaries between peace and war, but once its strategic objective, methods and implementation patterns acknowledged, it will not be hard to recognise the *"path of change"*.

Current national strategies (Defence and Military), operational concepts, doctrines and fighting manuals as well as the existing defence forces are not adapted to this composite of war. The same applies to *NATO's Strategic Concept* of 2010, Allied doctrines and concepts, already developed and tested, as well as to the *European Security Strategy* (2003) and the *European Union Treaty* (2009). As a result, defence and security organisations, member states and their armed forces may be considered unfit, both institutionally and intellectually, to meet the new challenges of hybridity.

To counteract these hybrid threats, in a more efficient way, all security and defence organisations and member states must better combine all elements of power in their campaign plans and strategic actions than they do today. Political, social, diplomatic and informational elements of power should provide full support for military structures. Leaders should encourage and provide the necessary resources for a Comprehensive Approach to deter conflicts through state actions, developing and preserving, at the same time, robust military capabilities to defend their vital interests. They should use all elements of power at their disposal to act indirectly, sometimes strengthening the capacity of partner governments and security forces to prevent crises before they become conflicts. This will help to isolate the threat, preparing, influencing and stabilising the international security environment through partnerships and global commitments.

Internally, governments need to improve inter-agency planning and integration to increase the capacity to address the non-military aspects of the conflict, by coordinating military efforts with those of the institutions that have responsibilities in the security and defence areas as well as by capitalising the expertise in the private sector, including NGOs and academia. Besides diplomatic and military powers, governments need to develop a more effectively integrated stabilisation and reconstruction capacity, ensuring the necessary resources and then coordinating efforts between civilian agencies and military services.

As a result, the approach to countering hybrid warfare should be integrated, comprehensive, civil-military, based on engaging all the elements of national power – diplomatic, informational, military and economic, inter-institutionally.

There are **some national measures** which need to be taken to counter such conflicts, as follows:

➢ establish an overall national strategy and implementation plan, to include responsibilities and preparatory measures for all institutions involved in countering this threat, comprising not only defence actions and military operations, but also security ones – political, social, economic, administrative, maintaining the rule of law and involving all the capabilities within the institutions participating in the conflict;

➢ establish the legal framework for inter-ministerial cooperation at political and expert level, as well as develop governmental decisions at ministerial level.

Establish Inter-Agency Working Groups, at experts' level, on operations planning issues and their sub-groups on different ministerial issues;

➢ develop and provide the necessary capabilities to counter such conflicts, in major areas (police, gendarmerie, civil protection, administration, justice) and provide differentiated specific training, together with military components.

For the latter proposed measure it is necessary to establish certain **operational requirements** able to define the need for further specific capabilities, such as: organisational flexibility; early warning through the collection of information; mobility, manageability and modularity, including in management structures; adaptability and flexibility; decentralised execution; simultaneity and continuity; rigour in the organisation and preparation of actions; initiative, speed and accuracy; use of cutting-edge technologies; actions in densely populated areas; a legal framework appropriate to participation.

In addition to the preparation of existing capabilities to face this new type of war, it would be advisable to **develop specific capabilities to counter hybrid war**, such as planning and preparing to counter/conduct Irregular Warfare (IW); Cyber Defence, Information Operations (INFO OPS); Strategic Communications (STRATCOM); Psychological Operations (PSYOPS), Civil-Military Operations (CIMIC); Special Operations Forces (SOF); Counterinsurgency Operations (COIN), and to assess them.

The development of these new specific capabilities to counter hybrid warfare can be achieved based on the following **courses of action**:

➢ ability to conduct and support multinational, joint and expeditionary operations, with limited or no host nation support, and to sustain national forces in theatres of operations for long periods of time, which entails the existence of joint bases, strategic transport, SOF, logistic management system, interoperability of C2 and logistic support;

➢ ability to conduct operations in difficult terrain and tough conditions by employing intelligence, surveillance, reconnaissance and early warning systems to achieve the common operational picture of the environment and to rapidly assess the situation;

➢ ability to adapt the forces structure, their deployment and mode of action in a fast and efficient manner, correlated with unforeseen circumstances – embarkation/disembarkation, force structure/modularity/flexibility, force protection and high-tech exploitation;

➢ ability and flexibility to conduct operations in a typical inter-institutional environment, which presupposes common legislation/legal issues and joint training and action.

In order to establish concrete measures to counter a potential hybrid war it will be necessary to clarify this new concept in relation to the changes the international security environment undertakes and to answer some questions that arise from the analysis of the crisis in Ukraine, as follows: *Is the Russian Federation capable to start a hybrid war against NATO? But against Romania? If yes, in what way – direct or indirect? In the indirect mode, which countries will be used as proxy – Hungary or the Republic of Moldova?*

Based on the certainty that the complex environment, in which a possible future conflict, be it conventional or hybrid, may be conducted, differs significantly from what we have known so far, the approach to the new conflict should be integrated, comprehensive, civil-military, by engaging all elements of national power – diplomatic, informational, military and economic, inter-institutionally. In this regard, we consider it beneficial to introduce elements defining the concept of hybrid warfare into main national strategic documents.

ELEMENTS OF HYBRID WARFARE IN THE ISLAMIC STATE OF IRAQ AND LEVANT OPERATIONS

Colonel Liviu IONIȚĂ
Lieutenant Colonel BEng Iulian AANIȚEI

The Islamic State of Iraq and the Levant (ISIL) has risen to prominence as a danger to peace and a regional threat with global impact. This perception comes, in large measure, from its successes in Syria followed by the rapid takeover of Northern Iraq. Its military victories are largely due to successful recruiting, intra-insurgent conflict, large cash reserves, as well as ineffective opponents.

As US President Barack Obama warned in September last year, ISIL represented a new type of challenge, a "sort of a hybrid of not just the terrorist network, but one with territorial ambitions, and some of the strategy and tactics of an army". Transnational aspirations, blended tactics, structured formations, propaganda and information warfare, and cruel use of terror as part of their arsenal reveal the hybrid nature of ISIL threat.

***Keywords**: ISIL; hybrid warfare; terrorism; threats; regional stability*

The enduring environment of deep mutual distrust and sectarian hatred still lingering in the Middle East as well as the highly biased and divisive policies carried out by the authorities in Damascus and Baghdad have fuelled tensions amongst various religious and ethnic communities in the area, with the hostility between Sunni and Shia as the prominent issue strongly impeding regional stability. The intense unrest in Syria and Iraq in the past years generated social, political and security vacuum that constituted fertile ground for a rapid growth of Sunni radicalism, which benefited from strong support from the local communities hostile to the authority. The prominent case in point is represented by the *Islamic State of Iraq and Levant (ISIL)* ascension. *ISIL* has rapidly evolved from a terrorist group mainly operating in Western Iraq to an advanced structured organisation

Colonel Liviu Ioniță, Lieutenant Colonel BEng Iulian Aaniței – experts on security matters within the Ministry of National Defence.

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

with a large operational and influence area, asserting itself as the main non-state threat to the regional stability and international security.

It is the USA that had the initiative to establish a wide *anti-ISIL* international coalition and over 60 states and international organisations currently back it. Subsequently, President Barack Obama presented the plan to counteract the threat posed by *ISIL*, aiming at the organisation's annihilation by a comprehensive and sustainable strategy to combat terrorism. In order for this aim to be achieved, the authorities in Washington focus on an internationally, regionally and locally integrated approach, through a wide array of military, law enforcement, economic and diplomatic means. This approach points out to the complexity of the issue and emphasises the hybrid nature of the threat posed by the terrorist organisation both regionally and internationally.

1. Ascension of the Islamic State of Iraq and Levant

1.1. The emergence and growth of the terrorist group

ISIL basis dates back in 1999, when Jordanian Abu Musab al-Zarqawi set up an extremist group, subsequently repositioned on Iraqi soil (in 2004, following the US intervention in Iraq). Its leader swore allegiance to al-Qaeda and rebranded the group as al-Qaeda in Iraq (AQI).

The establishment and growth of the group was favoured by the security and governance vacuum generated by the disintegration of Iraqi security forces and of Saddam Hussein's regime, against the background of an increasingly higher dissatisfaction of the Sunni community with the US-backed Shia Government in Baghdad. AQI was subsequently rebranded as the *Islamic State in Iraq (ISI)* and asserted itself as the central element of the Iraqi insurgency against the USA and its allies in Iraq.

The US withdrawal from Iraq (December 2011) and the biased and sectarian policies carried out by Shia Government led by Nouri al-Maliki fuelled *ISI* refreshment and terrorism in Iraq. The civil war that started in Syria (March 2011) created a fertile ground for ISI's expansion on Syrian soil, and led to the decision to rebrand *ISI* as *ISIL*.

ISIL has proved to be extremely efficient in Syria and succeeded in asserting its supremacy over other Syrian armed opposition groups and in controlling large territories in Northern and Western parts of the country. In June 2014, it launched a strong campaign in Northern Iraq and rapidly took control over large territories and important localities on Iraqi soil (Mosul and Tikrit). Amid significant operational successes, *ISIL* announced the establishment of the *Islamic "Caliphate"*, under the leadership of Abu Bakr al-Baghdadi (who proclaimed himself as Caliph Ibrahim)[1].

1.2. Organisation and capabilities

1.2.1. Leadership and business management

ISIL has evolved from an exclusively combat-oriented force to an advanced structured organisation able to govern over controlled territories, where the political decision-making process and the military command and control process are interrelated. The system is based on a bureaucratic hierarchy which is broadly similar to the one of Western states (whose values are, however, rejected by the group)[2].

Abu Bakr al-Baghdadi, the leader of *ISIL*, together with his advising team and his two deputies (for the Syrian and Iraqi affairs, respectively), represents the central executive power, known as *"Al Imara"*. Al Baghdadi's religious past and his degree of Doctor in Islamic Studies he reportedly got from the Islamic University in Baghdad give the organisation a relatively high status of Islamic legitimacy. The Shura Council reports directly to the executive power and it is responsible for the religious affairs, including to supervise that local governments and councils observe the Sharia law version fostered by *ISIL*. At the same time, it monitors the leadership activity in order to provide for the proper enactment of religious standards. In the areas under its control, the organisation established alternative administration systems to the official ones (Iraqi and Syrian). They include educational, law enforcement, police and judicial networks, and aim to provide services and impose Salafi-jihadist ideology on population.

1.2.2. Military capabilities

ISIL has a significant arsenal of weapons and military equipment at its disposal, with the large majority of pieces seized from the Iraqi and Syrian military bases and facilities it captured. They include tactical equipment, Infantry small arms, rocket propelled grenades and mortar shells, anti-tank and air-defence rockets, light tactical and logistical transportation vehicles. Additionally, *ISIL* uses heavy weapons and other types of military equipment which is normally intended

[1] Aaron Y. Zelin, *Abu Bakr al-Baghdadi: Islamic State's Driving Force*, Washington Institute for Near East Policy, 31.07.2014, see BBC News, http://www.bbc.com/news/world-middle-east-28560449, retrieved on 03.02.2015.

[2] Nick Thompson and Atika Shubert, *The Anatomy of ISIS: How the 'Islamic State' Is Run, from Oil to Beheadings*, 14.01.2015, see CNN News, http://edition.cnn.com/2014/09/18/world/meast/isis-syria-iraq-hierarchy, retrieved on 03.02.2015.

for regular armed forces – artillery, machine-guns and man-portable air defence systems (MANPADS), tanks and other armoured vehicles.

The organisation's strengths are estimated between 20,000 to 31,000 fighters[3], including approximately 15,000 foreign fighters originating from European states, Africa, Central and Eastern Asia, Russian Federation, Canada, USA, Australia.

1.2.3. Areas under control of ISIL. Financial resources

At the end of November 2014, one third of the Iraqi soil and one quarter to one third of the Syrian soil were under *ISIL* control, stretching from the Eastern outskirts of Syrian town Aleppo to the proximity of the Iraqi capital city of Baghdad. According to estimates, the population of these areas reaches six to eight million. At the same time, other important localities are under ISIL control, including Mosul (second largest city in Iraq), Fallujah (symbol of the fight against the US presence in Iraq), Ar Raqqah (stated *"capital"* of ISIL, in the Northern part of Syria) and Deir Az Zowr (in the Western part of Syria).

Financially, *ISIL* has manifold sources of income, leading to self-sufficiency and thus the capability to establish its own agenda and support its implementation. Accordingly, *ISIL* has seized extraordinary capabilities and financial resources which allow it to sustain military operations and establish a functional governmental and administrative system.

Oil and oil-based products generate the most considerable funds for *ISIL*. During its actions on Syrian and Iraqi soil, *ISIL* has seized control of important national infrastructure objectives, and it has commandeered a large part of Syrian oil fields and, to a lesser extent, of Iraqi[4] oil fields.

According to estimates, the revenues originating in oil and oil-based products commerce last autumn reached approximately USD three million[5]. *Nevertheless, they considerably reduced due to the International Coalition's air strikes which targeted oil infrastructure.*

Robbing banks (including Mosul Central Bank) and gold shops has been another significant means of financing. Also, *ISIL* has routinely practiced blackmail and extortion[6], seizing displaced individuals' real estates, demanding fees

[3] *"IS Has 20,000–31,500 Fighters in Iraq and Syria: CIA"*. Yahoo! News, 12.09.2014.

[4] Ben Hubbard and Eric Schmitt, *Military Skill and Terrorist Technique Fuel Success of ISIS*, 27.08.2014, *The New York Times*, see http://www.nytimes.com/2014/08/28/world/middleeast/army-know-how-seen-as-factor-in-isis-successes.html, retrieved on 30.01.2015.

[5] *Ibidem*.

[6] *How ISIS Works*, *The New York Times* online, 16.09.2014, see http://www.nytimes.com/interactive/2014/09/16/world/middleeast/how-isis-works.html, retrieved on 05.02.2015.

(for transit, protection etc.), weapon and supply trafficking, and it has widely received *"sponsorship"* and funding from private donors in Gulf States[7].

2. The Hybrid Dimension of ISIL Actions

2.1. ISIL as a hybrid threat

Over the past years, *ISIL* has considerably expanded its operations and influence area through a deliberate and methodically approached strategy that involved, among other matters, fuelling the sectarian conflict, exploiting the domestic policy weaknesses, and fully and brutally exerting military power.

Even if its fundamental structure stays similar to the one of a terrorist organisation, *ISIL* expansion and objectives are much more advanced, aiming at establishing and securing an efficient proto-state on Syrian and Iraqi soils. Militarily, the group has proved capable of fighting both as light infantry forces, with heavy fire support, and as guerrilla-type forces that blend in densely populated areas where they get engaged in combat. Under these circumstances, *ISIL* should be approached as an entity whose *"modus operandi"* differs significantly from the one of a terrorist organisation.

Since 2010, it is likely that *ISIL* has evolved from a terrorist group to a *"viable armed force"* whose general strategy to strengthen and expand the Caliphate has *"fundamentally relied on its military superiority in order to seize control over territories and localities of modern states"*[8]. Consequently, *ISIL* should not be seen and analysed as a terrorist group exclusively, but as a hybrid threat. This statement is backed and justified by the hybrid nature of its features and its *"modus operandi"*, which involve, among others[9]:

- *Combined tactics*: the group combines asymmetric-type activism (terrorist bombings, and *"hit & run"* guerrilla tactics) with conventional posture confrontation.
- *Flexibility and adaptability*: the group has paramilitary forces able to organise and operate both in large conventional units and in small formations.

[7] Jacob Shapiro, *Smuggling, Syria, and Spending*, in *Bombers, Bank Accounts, and Bleedout: Al-Qa'ida's Road In and Out of Iraq*, Combat Terrorist Centre at West Point, 22.07.2008, see http://www.juancole.com/2008/08/ctc-west-point-al-qaidahs-road-in-and.html, retrieved on 05.02.2015.

[8] Jessica Lewis, *The Islamic State: A Counter-Strategy for a Counter-State*, Institute for the Study of War, July 2014, see http://www.understandingwar.org/report/islamic-state-counter-strategy-counter-state, retrieved on 06.02.2015.

[9] Scott Jasper and Scott Moreland, *The Islamic State Is a Hybrid Threat: Why Does That Matter?*, Small Wars Journal, 01.12.2014, see http://smallwarsjournal.com/ jrnl/art/the-islamic-state-is-a-hybrid-threat-why-does-that-matter, retrieved on 03.02.2015.

- *Control and administration of territories*: the group has a governmental body which maintains stability in the territories under control and support the group's operations.
- *Propaganda campaign and information operations*: the group exploits global communication networks in order to promote its values and jihadi ideology, to radicalise, to recruit, and to collect funds.
- *Terrorism*: the group relies on terrorist actions in order to instil terror and despair, and to set fear and panic into foes.
- *Functioning as a criminal enterprise*: it uses criminal activities in order to obtain resources needed to fund its combat operations, its recruiting and training process, and also to support its governmental power.

The main feature of *ISIL* hybrid dimension is *its ability to engage complex combat operations, by combining conventional tactics, techniques, procedures, and capabilities with asymmetric attacks*. This characteristic manifested during the past years developments and especially during the offensive in Iraq, in the summer of 2014.

2.2. Conventional and unconventional in ISIL's activity

The offensive in Iraq in the summer of 2014 may by understood in the larger context of *ISIL* political and military campaigns in the past five years, and especially in May 2010 when *ISIL* was practically reset under the leadership of Abu Bakr al-Baghdadi[10]. Since then, *ISIL* has gradually and continuously strengthened its power and has soundly planned the future operational environment. Al-Baghdadi made use of the years before 2014 to build up a strong army and simultaneously weaken Iraqi security forces. *ISIL* benefited from the US forces' withdrawal from Iraq and from the civil war in Syria in order to establish safe havens and refresh its suicide attackers' network. Since 2012, *ISIL* has built up well trained and highly motivated light infantry forces that accumulated combat experience both during the war in Syria and from former jihadists who participated in the Balkans' and Chechnya's wars[11]. At the same time, al-Baghdadi established and developed a very efficient command and control system, based on the principle of *"centralised command, decentralised execution"*.

[10] Murad Batal al-Shishani, *The Islamic State's Strategic and Tactical Plan for Iraq*, in *Terrorism Monitor*, 2014, The Jamestown Foundation, see http://www.jamestown.org/programs/tm/single, retrieved on 12.02.2015.

[11] Douglas Ollivant and Brian Fishman, *State of Jihad: The Reality of the Islamic State in Iraq and Syria*, War on the Rocks, 21.05.2014, see http://warontherocks.com/2014/05/state-of-jihad-the-reality-of-the-islamic-state-in-iraq-and-syria/, retrieved on 10.02.2015.

Through its actions, *ISIL* has proved its ability to organise, deploy and engage conventional forces into combat. This major combat capability has been supported by small-sized elements and asymmetric-type tactics which allow *ISIL* to rapidly adapt to the tactical environment and to reduce own forces' vulnerabilities to enemy air strikes and counter-offensive.

In June 2014, ISIL launched a powerful offensive on Iraq, and attacked Mosul with a main striking force of 500 to 800 fighters deployed on Syrian soil[12]*. ISIL applied an efficient strategy of expansion succeeding in deliberately isolating, in some cases, part of the Iraqi security forces, and advanced towards Baghdad simultaneously from North and West. The actions were supported by a robust conventional firepower and very high mobility, leading to ISIL shortly taking control over important urban centres, lines of communication and large territories in Iraq.*

When *ISIL* offensive was slowed down and ultimately stopped due to the International Coalition's air strikes, jihadists adapted to the new environment and dispersed their strengths and their combat equipment in populated centres, where they mainly operated during night and re-distributed forces into small tactical elements, by simultaneously limiting radio and unsecured mobile phones communications[13].

At the same time, *ISIL* laid down mines and IEDs in order to limit and even prevent Iraqi and Peshmerga Kurdish forces' freedom of movement, during their operations. Mines and IEDs have proved to be very efficient means to passively defend areas of interest, since these means are not vulnerable to air strikes. Additionally, the process to neutralise these devices is very difficult and involves demining procedures which are extremely dangerous for the personnel who carry them out. *ISIL* uses drones for air reconnaissance missions, and several other types of equipment previously seized during offensive actions, as for example Infantry Fighting Vehicles, Artillery pieces and Infantry arms. Recent evidence points out to the fact that jihadists used chemical agents during the offensive launched against the Iraqi city of Dhuluiya[14] in October 2014.

[12] Jessica Lewis, *The ISIS Battle Plan for Baghdad*, Institute for the Study of War, 27.06.2014, see http://www.understandingwar.org/backgrounder/isis-battle-plan-baghdad, retrieved on 09.02.2015.

[13] Nour Malas, Dion Nissenbaum and Maria Abi-Habib, *US-led Airstrikes Disrupt Islamic State, but Extremists Hold Territory*, in *The Wall Street Journal*, 5 October 2014, see http://www.wsj.com/articles/u-s-led-airstrikes-disrupt-islamic-state-but-extremists-hold-territory-1412555718, retrieved on 08.02.2015.

[14] Tamer El-Ghobashy and Ghassan Adnan, *Iraqi Officials Say Islamic Militants Used Chlorine Gas North of Baghdad*, in *The Wall Street Journal*, 24 October 2014, see http://www.wsj.com/articles/iraqi-officials-say-islamic-militants-used-chlorine-gas-north-of-baghdad-1414164016.

2.3 Tactics, techniques and procedures used during offensive operations

ISIL has gained major operational successes mostly due to high manoeuvrability and surprise of the adversary during conventional warfare operations. When it comes to analysing the offensive operations conducted by *ISIL* in Iraq during the summer of 2014, the main characteristics of the operations were forces' manoeuvrability and tactical surprise of the attacked forces (Iraqi and Kurdish). They were achieved through marches and quick deployment of forces, using the high quality and dense land communication networks, culminating with night or early in the morning raids[15]. *ISIL* ability to concentrate equipment and troops nearby the target was possible because of the local security forces lack of night vision equipment, as well as of the poor analysis of the battlefield situation and tactical intelligence.

Due to its high mobility and deception techniques, *ISIL* often managed to reach superiority of forces against local security forces, even if generally speaking *ISIL* forces compared to governmental security forces were much smaller in terms of personnel and equipment.

At the same time, reconnaissance, small engagements and diversion tactics have been repeatedly used in offensive operations in order to identify security forces' readiness and reaction procedures, avoiding security forces' strong points and misguiding them from the main target. One such situation occurred during the attack on the city of Jalula (10.08.2014) when *ISIL* forces managed to take control of the city by simulating an attack on a nearby city (Makhmour) forcing the Kurdish troops to deploy to the respective area.

Once *ISIL* forces seized a significant number of armoured vehicles, it used those vehicles as part of own battle groups (2 to 5 vehicles per battle group) in order to increase fire power. Occasionally, armoured vehicles were used as part of the psychological warfare conducted by *ISIL* aiming at surprising the enemy and inflicting it with a profound feeling of fear and helplessness (the so called *"tank fear"* effect).

Artillery means have been used during offensive operations in order to attack enemy defensive positions and weaken its capabilities. Such situation occurred during the siege on Zummar and Kisik (West of Mossul) or Zowiya (according to estimates nearly 500 shells were fired on the targets)[16].

[15] Lauren Squires and Nichole Dicharry, *Iraq Situation Report: 13 August 2014*, Institute for the Study of War, 21.08.2014, see http://iswiraq.blogspot.ro/2014/08/iraq-situation-report-august-13-2014.html, retrieved on 11.02.2015.

[16] Mohammed al-Dulaimy and Hannah Allam, *Witnesses Describe How Islamists Leveled Sunni Village as a Warning*, McClatchy Newspapers, 11.07.2014, see http://www.mcclatchydc.com/2014/07/ 11/ 233107/witnesses-describe-how-islamists.html, retrieved on 10.02.2015.

When *ISIL* leadership aims at instilling panic and destabilising the enemy defensive system, most of the time the offensive is initiated by several IED attacks against local security forces' HQs and checkpoints, inflicting a high number of casualties. This *"modus operandi"* was established in 2010 and it has been improved ever since; one of the first attacks of this kind took place in June 2010, in Baghdad, against several police checkpoints within Adamiyah area[17].

Since summer 2011, the number of such attacks have significantly increased, and *ISIL* has improved its *"modus operandi"* by using vehicle-borne IEDs (VBIEDs) in order to create more chaos and breaches within the security perimeters providing the opportunity for suicide attackers or armed fighters (dressed in local security combat uniforms) to penetrate the objectives[18] and inflict more casualties.

ISIL forces regularly use a wide variety of extreme violence during their offensive operations – *"strategic killings"* according to some experts – in order to instil fear and terror amongst local security forces and inhabitants[19]. On 11.06.2014, in Tikrit, *ISIL* fighters killed nearly 100 local security forces members because they refused to join *ISIL*; this mass killing had a high media profile and it was used as an example of what would happen to Iraqi soldiers if they stand against *ISIL*[20].

2.4 Tactics, techniques and procedures used during defensive operations

Defending the areas under *ISIL* control has posed a major challenge for its fighters. Before the establishment of the *"Caliphate"*, *ISIL* could lose controlled areas without damaging its prestige[21]. Subsequently, in order to *"validate its statehood, ISIL had to prove that it could defend its territory or deter an outside attack"*[22]. Having this in mind and taking into consideration small scale counter-attacks conducted by Iraqi security forces, *ISIL* has proved that it is able to adapt

[17] Iraqi Quick Reaction Forces on route to the attacked checkpoints were engaged by several IEDs located along the road. These IED attacks caused at least 23 deaths among security forces and had a high media profile. See Michael Knights, *Back with a Vengeance: Al-Qaeda in Iraq Rebounds,* in *IHS Defense, Security & Risk Consulting*, see http://more.ihs.com/IHSJanesDefense?retURL=http%2FThe_Islamic_State_expands_its_influence_in_Asia, retrieved on 10.02.2015.

[18] Michael Knights, *op. cit.*

[19] Robert Scales and Douglas Ollivant, *op. cit.*

[20] Sarah Leah Whitson, *Iraq: ISIS Abducting, Killing, Expelling Minorities: Armed Group Targeting Christian Nuns, Turkmen, Shabaks, Yazidis,* Human Rights Watch, 19.07.2014. see http://www.hrw.org/news/2014/07/19/iraq-isis-abducting-killing-expelling-minorities, retrieved on 10.02.2015, and Damien McElroy, *Islamic State Jihadists Issue 30-Minute Killing Spree on Video*, in *Daily Telegraph*, 30.07.2014, see http://www.telegraph.co.uk/news/worldnews/middleeast/syria/11000079/Islamic-State-jihadists-issue-30-minute-killing-spree-on-video.html, retrieved on 10.02.2015.

[21] J.M. Berger, *Gambling on the Caliphate*, Intelwire blog, 29.06.2014, see http://news.intelwire.com/2014/06/gambling-on-caliphate.htm, retrieved on 11.02.2015.

[22] Jessica D. Lewis, *op. cit.*, footnote 12.

to the operational environment and possesses good defensive capabilities, which highlights once again the hybrid nature of *ISIL* operations.

ISIL has regularly adopted an area defensive strategy that involves complex tactics, techniques and procedures. One significant example in this regard is represented by the defensive strategy established for the protection of Mossul dam (August 2014) when *ISIL* used the inhabited areas around the dam and a wide variety of forces ranging from tactical units to paramilitary groups. The defensive measures also involved armoured vehicles and artillery pieces. During the operation, *ISIL* conducted intense information warfare that included threatening messages against Iraqi security forces, claiming that all Iraqi units would be destroyed and offensive operations would be extended to the respective units' area of origin. Placing obstacles and IEDs along the avenues of approach managed to slow the advancement of security forces and blocked them into key terrain *("kill zones")*, providing the defending forces with the possibility to engage the advancing forces with direct fire. *ISIL* maintained a high level of readiness by organising numerous harassing attacks (ambushes and small scale engagements) and using light weapons (including rocket propelled grenades – RPGs), non-tactical vehicles (NTVs) equipped with heavy weapons, or even armoured vehicles. Moreover, *ISIL* used successfully on a large scale concealment, cover, hiding and diversion techniques. During battle preparations *ISIL* established Quick Reaction Forces in certain areas, designated to operate according to the battlefield situation.

Area defensive strategy consisted of:

- use of qualified personnel and equipment for engineering preparations and minefields emplacing along the most probable enemy counter-attack avenues of approach;

After taking control of Jalula City (11.08.2014), ISIL fighters established a defensive perimeter using ditches and dirt obstacles, blocking this way the options for Kurdish counter-offensive. Additionally, they placed IEDs along the main ground communications[23]*. Later on ISIL defenders destroyed the bridge over the Diyala River between Jalula and Kalar. This tactic of destroying bridges and altering the terrain is a tactic often used by ISIL in order to limit counter-attacks or deployment of additional troops.*

- strong defensive points enclosing anti-tank weapons (RPG or anti-tank missile launchers) supported by tanks (T-55 or T-62) and light weapons[24];
- ambushes and counter-attacks, using high mobility and well equipped forces.

[23] Isabel Coles, *Purge of Minorities Re-draws Iraq Map*, Reuters, 24.07.2014, see http://in.reuters.com/article/2014/07/24/uk-iraq-security-minorities-idINKBN0FT1IJ20140724, retrieved on 12.02.2015.

[24] Brown Moses, *ISIS Deploys Croatian Weapons against the Iraqi Army*, Brown Moses Blog, 08.03.2014, see http://brown-moses.blogspot.ro/2014/03/isis-deploys-croatian-weapons-against.html, retrieved on 12.02.2015.

As a result of taking control over some military bases and weapons depots belonging to Iraqi and Syrian armed forces, and also due to the support provided by some international actors, *ISIL* managed to obtain air defence capabilities. Currently, it is possible that *ISIL* units use a small number of air defence systems such as ZU-23s, FN-6, SA-7s and SA-16s[25]. The capabilities of such systems consist of 6 km range and 4.5 km altitude. Taking into consideration the limited number of such systems available to *ISIL* it is highly probable that they will be used for the defence of major urban areas or *ISIL* safe havens[26]. In order to defend these areas it is possible that *ISIL* will use multiple systems and a high rate of fire.

During defensive operations, *ISIL* uses air defence systems integrated within complex combat positions, combined with several types of forces and equipment, in order to protect its personnel and equipment, limit the enemy freedom of movement, control the area or buy time.

After ISIL took control of Jalula city (11.08.2014), it organised a defensive establishment comprising of T-55 and T-62 tanks, anti-tank weapons and recoilless guns in order to protect ground avenues of approach towards the city[27].

3. Conclusions

Past decades events in the Middle East and Northern Africa have highlighted an uneven development of threats, at first of asymmetrical nature, genuinely transnational, followed by a mixture of unconventional happenings with hybrid attributes. Non-state actors, previously acting in an independent manner, have joined efforts to achieve strategic surprise as well as physical and psychical superiority. A case in point is the area of Iraq-Syria where autonomous or traditionalist terrorist entities operate under the banner of the Islamic State, being able to survive to attacks from a military conventional apparatus.

The current situation in Iraq-Syria is a significant threat to the West. As for the threats to the security of Europe, they are increasingly generated along a vertical axis: migrants, traffickers and terrorists who use the Mediterranean Sea as a transit route to the European Union. The emergence of training bases and refuge areas within the territories controlled by *ISIL* in Iraq and Libya,

[25] Jake Bierbaum, *ISIL Background and Fighting Techniques*, National Ground Intelligence Center (NGIC), 12.09.2014.

[26] *Islamic State: An Assessment of Capabilities and the Effectiveness of International Intervention*, IHS Jane's, 30 October 2014, see http://www.janes.com/events, retrieved on 12.02.2015.

[27] Michael Knights, *ISIL's Political-Military Power in Iraq,* West Point Combating Terrorism Center: CTC Sentinel, 27.08.2014, see https://www.ctc.usma.edu/posts/isils-political-military-power-in-iraq, retrieved on 11.02.2015.

designated for those who conduct terrorist acts in Europe, serves as a reminder of this threat, especially after Paris and Copenhagen attacks. The decline in the power of the authoritarian regimes that previously contributed to guaranteeing security, partially as a result of the *Arab Spring*, has eliminated part of the defence lines which formerly protected NATO Southern and Western members and put more responsibilities on the first line European states[28].

The main issue the international community has faced ever since the so called *"Iraqi invasion"* (2003) is the conventional approach to an asymmetric threat, leading to no results but an increase in the instability area and new conflict causes. Against a backdrop of widening gaps between the two cultures and civilisations (Arab and Western), the jihadist entities from the Middle East have grown and attracted sympathisers from all over the world, people who, for various reasons, were frustrated or dissatisfied with the societies they lived in.

Even if the conventional component of *ISIL* makes the organisation more vulnerable, being predictable and exposing its identity, the hybrid nature of *ISIL* operations widens its area of presence and fuels its capability to generate global risks and threats.

[28] Nikolas Gvosdev, *Crises in Ukraine, Libya Confront NATO with Risk of Division*, in The World Politics Review, 18.02.2015, see http://www.worldpoliticsreview.com/articles/15106/crises-in-ukraine-libya-confront-nato-with-risk-of-division, retrieved on 19.02.2015.

THE ROLE OF THE EUROPEAN UNION IN CONFLICT RESOLUTION IN UKRAINE

Dr Mihaiela BUŞE

The European Union (EU) is a regional player that aims to strengthen its global status by becoming involved more actively and effectively in maintaining peace and stability in the world. In the EU vision, conflict resolution methods should be peaceful, the organisation choosing to respond to violence through mediation and dialogue and not through military force. Since the beginning of the conflict in Ukraine, the EU has sent its representatives to assist it in the difficult situations it has been experiencing. Various instruments have been involved in solving the crisis, such as restrictive, diplomatic, economic measures merged with mediating and facilitating dialogue.

***Keywords**: conflict resolution; European Union; Ukraine; mediation; dialogue*

1. UN Charter – Cornerstone of Conflict Resolution Methods

Conflict resolution is a relatively new field. However, the armed conflicts and wars have a rich history. The two world wars shook the world so much that mankind wanted a period of peace, harmony and understanding between peoples. Thus was established the United Nations, whose declared aim is to maintain international peace and security and which is based on the UN Charter. The starting point for violent conflicts resolution should be the UN Charter, which mentions two ways of resolving conflicts: on the one hand, peaceful ways, on the other hand – under certain conditions –, the use of force.

Peaceful methods for violent conflicts resolution

Chapter VI of the UN Charter presents the peaceful methods for dispute settlement – negotiation, enquiry, mediation, conciliation, arbitration,

Dr Mihaiela Buşe – lecturer, *"Carol I"* National Defence University, Bucureşti.

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

judicial settlement, resort to regional agencies or arrangements, or other peaceful means –, which are recommended to be used in a spirit of tolerance and good coexistence among peoples.

The use of force as a means to resolve violent conflicts

In Chapter VII of the UN Charter two situations are provided when armed force can be used. Firstly, it stipulates that where prevention and constraint measures taken against a state do not have the desired result, the Security Council *"may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security. Such action may include demonstrations, blockade, and other operations by air, sea, or land forces of Members of the United Nations"*[1]. Secondly, Article 51 provides that if an armed attack occurs against a UN member state, it can exercise the right to individual self-defence, being allowed to use military force in response to the aggression to which it has been subjected.

Conflict resolution is mainly the preserve of supranational construction. Among the important mediators are the UN, the EU, OSCE and the African Union. The USA also enjoys the status of mediator as a world great power. It should be also noted the recent initiative of Germany and France in the Minsk negotiations to conclude a peace agreement on the conflict in Ukraine.

2. The Resolution of Violent Conflicts from the European Union Perspective

The Union's external action is based on democracy, rule of law, universality and indivisibility of human rights and fundamental freedoms, respect for human dignity, principles of equality and solidarity, as well as the principles of the UN Charter and the international law[2]. These principles also lie at the basis of the EU establishment and development. According to the *Treaty on the European Union*, the Council and the Commission, assisted by the EU High Representative for Foreign Affairs and Security Policy, ensure the coherence between different domains of the EU external action and its policies.

Since 2011, the EU has a diplomatic service created by the Treaty of Lisbon as the European External Action Service (EEAS). EEAS and implicitly the European diplomacy are led by the High Representative for Foreign Affairs and Security Policy, the only voice of the 28 member states and the EU diplomacy chief.

[1] ***, *Charter of the United Nations*, Chapter VII: Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression, Article 42, see http://www.un.org/en/documents/charter/chapter7.shtml, retrieved on 16 February 2015.

[2] *Treaty on the European Union* (consolidated version), see http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012M/TXT.

As a promoter of peace, democracy and human rights, the EU has all the makings to set itself up as a mediator to pave the way for peace and stability. Mediation is the most used method in diplomacy within the EU to facilitate conflict resolution. In this respect, the EU contribution concerning the settlement of the Israeli-Palestinian conflict, the dialogue between Belgrade and Pristina, and the efforts to end the Six-Day War in Georgia are eloquent evidence of the EU experience in this field.

Although the EU mediation experience was rich, it was considered necessary to take measures to increase the capacity of mediation and dialogue so, on 3 November 2009, the *Concept on Strengthening EU Mediation and Dialogue Capacities* was adopted. For the European Council and the European Commission, the concept is *"a policy basis for EU engagement in the area of mediation and dialogue"*[3]. The EU involvement in mediation and dialogue can be found in both the *European Security Strategy (2003)* and the report on its implementation (2008), all prepared under the direction of Javier Solana, the EU High Representative for the Common Foreign and Security Policy (CFSP) at the time.

From the EU perspective, ***mediation*** is an effective and relatively inexpensive tool that can be used successfully not only in conflict prevention but also in conflict transformation and resolution. In this respect, the EU concept on mediation activity and the implementation of peace agreements resulted in a comprehensive approach involving support through a wide range of civilian and military instruments for crisis management as well as through trade and development specific instruments. Regarding the role of a mediator, the High Representative (HR), the Presidency, the European Commission, EU Special Representatives and European Commission delegations can undertake mediation actions within the EU.

The proposed concrete measures meant to strengthen the capacity of the EU in the area of mediation cover several directions: strategic aspects, operational support, training, knowledge management, outreach and cooperation. Among the measures set out in the *Concept on Strengthening EU Mediation and Dialogue Capacities* we mention: the EU mediation activity carried out by its representatives with expertise in this area should materialise in an early stage of the conflict; the EU must act as a binder at diplomatic level and at the same time financially intervene to support the mediation process; the EU must provide specialised training to its actors involved in the mediation process; the exchange of experience and best practices of mediators are encouraged and it is required to strengthen cooperation with international partners.

[3] Conseil de l'Union européenne, *Concept relatif au renforcement des capacités de l'UE dans le domaine de la médiation et du dialogue*, Brussels, 3 November 2009, see http://eeas.europa.eu/cfsp/conflict_prevention/docs/ening_eu_med_fr.pdf, retrieved on 12 February 2015.

The vast experience of the EU as a mediator has opened new perspectives in the mediation approach, the EU contributing significantly to the development of important aspects of mediation by: promoting mediation as a peaceful method of resolving tensions and conflicts; supporting mediation by tools specific to different domains – civilian and military instruments for crisis management, and trade and development instruments; providing assistance in mediation in terms of training, logistical support and expertise provided to both the mediator and the parties to the conflict; financially supporting the mediation process. The consolidation of the support capacity in the mediation and dialogue field will enable the EU to have a considerably greater role in the efforts directed towards conflict prevention and resolution.

A complementary instrument is the *Mediation Support Team*, which provides expert support in the area of mediation and dialogue to the EU institutions, its partners and EU representatives that are active in many parts of the world: Mali, Myanmar, Yemen, Lebanon, Syria, Middle East, North Africa, Afghanistan, South Caucasus, Central Asia, Western Balkans, Zimbabwe, Kenya, Nigeria, Central America[4]. This team was established within the European External Action Service in 2011 in order to provide technical expertise, advice, and operational support[5] and to address the need for the consolidation of the EU support capacity in the mediation and dialogue field.

3. The EU Approaches to Resolving the Conflict in Ukraine

The annexation of Crimea by the Russian Federation on 16 March 2014 marked the first step in Vladimir Putin's bold plan to restore Russia's domination on the states from the former USSR. This fact has generated, in addition to the dismay and condemnation from the international community, a serious diplomatic crisis. The European Parliament took action on 13 March 2014 by asking Russia to withdraw its military forces from Ukraine. Crimea was attached, and the EU response to this action that threatened the territorial integrity of Ukraine was extremely fast: the day after the annexation of Crimea by the Russian Federation there were adopted restrictive measures[6] against those responsible for undermining

[4] Union européenne. Action extérieure, *Équipe de soutien à la médiation de l'UE*, see http://www.eeas.europa.eu/cfsp/conflict_prevention/docs/2013_eu_mst_factsheet_fr.pdf, retrieved on 14 February 2015.

[5] European Union External Action, *Fiche technique, Équipe de soutien à la médiation de l'UE*, see http://eeas.europa.eu/factsheets/docs/factsheet_eu-mediation-support-team_fr.pdf, retrieved on 14 February 2015.

[6] Council of the European Union, *EU Adopts Restrictive Measures against Actions Threatening Ukraine's Territorial Integrity*, Brussels, 17 March 2014, see http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/141603.pdf, retrieved on 17 February 2015.

or threatening the Ukrainian territorial integrity, sovereignty and independence, consisting of imposing travel restrictions and assets freeze measures. A few days later, on 21 March, the EU decided to extend the restrictive measures[7] related to travelling by adding other persons to the existing list, followed by a cascade of restrictive measures for people from Russia and Ukraine, Russian entities, Crimea and Sevastopol (12 May, 28 May, 11 July, 18 July, 24 July, 25 July, 29 July, 30 July, 31 July, 11 September, 28 November, 18 December 2014).

The second phase of Putin's plan materialised in a short time by taking control over the state institutions by the pro-Russians demonstrators in the cities of Harkov, Donetsk and Lugansk located in Eastern Ukraine. The success of pro-Russian separatists resulted in accusations, at international level, regarding their covert support. Both Ukraine and Western countries drew attention to the fact that the Russian Federation provided pro-Russian separatists with troops and equipment. Following the Crimean model, which was based on the Kosovo precedent, on 11 May, a referendum was organised, and Donetsk and Lugansk were declared independent. Such destabilising actions that affected the territorial integrity of Ukraine were denounced by Ukraine as being caused by the Russian Federation. Ukraine conducted an anti-terrorist operation in the areas where pro-Russians separatists acted, but the powerful military equipment in their possession and their military training had the effect of gradual withdrawal of the Ukrainian army and therefore the continuing loss of land, numerous civilian casualties and an increasing number of people who, for fear of armed battles, left their homes and lifetime possessions to save themselves.

An element with a deep emotional charge in the Ukraine crisis was the *Malaysia Airlines Boeing 777* plane crash, on 17 July 2014, in the Ukrainian region of Donetsk controlled by pro-Russian separatists, where violent clashes between them and the Ukrainian army were conducted. The plane had taken off from Amsterdam bound for Kuala Lumpur. Both Ukraine and the Russian Federation accused each other for shooting down the plane that caused the deaths of all 288 people on board. According to *Der Spiegel* cited by Mediafax, the German Foreign Intelligence Service found that the plane *"was shot down by pro-Russian insurgents with a missile system stolen from the Ukrainian army"*[8]. Following this aviation tragedy the EU imposed new sanctions.

[7] Council of the European Union, *EU Strengthens Sanctions against Actions Undermining Ukraine's Territorial Integrity*, 21 March 2014, see http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/141741.pdf, retrieved on 17 February 2015.

[8] Mihai Drăghici, *Raport privind zborul MH17: Avionul prăbuşit în Ucraina, doborât de proruşi cu un sistem luat de la armata ucraineană. Rebelii resping acuzaţiile*, Berlin, 19 October 2014, see http://www.mediafax.ro/externe/nou-raport-privind-zborul-mh17-avionul-prabusit-in-ucraina-doborat-de-prorusi-cu-un-sistem-luat-de-la-armata-ucraineana-rebelii-resping-acuzatiile-13415452, retrieved on 17 February 2015.

On 29 July 2014[9] the EU set up economic sanctions and diplomatic measures against the Russian Federation. The economic sanctions took into account two distinct aspects: on the one hand, Russia's restricting access to the capital markets in the EU and, on the other hand, imposing embargo on the import and export of weapons and related materiel from and to the Russian Federation. The diplomatic measures taken against the Russian Federation were aimed at isolating and restricting access to international organisations. In this context, a G7 meeting in Brussels was preferred, on 4 and 5 June 2014, to the G8 summit that was to be held in Sochi. The EU also decided to suspend negotiations on Russia's accession to the Organisation for Economic Cooperation and Development (OECD) and the International Energy Agency and to cancel the EU-Russia summit.

The G-7 Leaders' Statement on Ukraine, on 30 July 2014, states the openness to finding a political solution to end the ongoing conflict. Moreover, a peaceful settlement of the crisis in Ukraine is required and the warring parties are asked to conclude a ceasefire agreement as soon as possible. The G-7 leaders also requested the Russian Federation help in two situations: to make use of its influence on pro-Russian separatists and to ensure an efficient border control with the help of OSCE observers.

On 11 August, the European Commission President, José Manuel Durão Barroso had phone conversations on the situation in Ukraine with both President Poroshenko and President Vladimir Putin. The conversation with President Poroshenko focused on the humanitarian aid needed by Ukraine. President Barroso met the demand of Ukrainian President informing him that he would urgently adopt a decision on additional humanitarian assistance within the international intervention plan initiated by the United Nations Organisation.

Indeed, the second day after the phone conversation between President Barroso and President Poroshenko, the European Commission offered a further humanitarian aid of 2.5 million EUR to Ukraine to assist the people affected by conflict in the East of the country. The allocation of the funds was intended *"to register and relocate internally displaced people (IDPs), provide shelter, food, water, healthcare, psycho-social assistance and protection in preparation for the coming winter"*[10]. This prompt financial aid from the EU to the Ukrainian civilian population was possible because of the values shared by the member states and especially

[9] Council of the European Union, *EU Restrictive Measures in View of the Situation in Eastern Ukraine and the Illegal Annexation of Crimea*, Brussels, 29 July 2014, see http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/144159.pdf, retrieved on 17 February 2015.

[10] European Commission, *EU Increases Humanitarian Assistance for Ukrainian Conflict-affected Population,* Brussels, 12 August 2014, see on http://europa.eu/rapid/press-release_IP-14-924_en.htm, retrieved on 17 February 2015.

because of the EU status as main donor of humanitarian aid worldwide. It was not the only financial aid provided to Ukraine by the EU.

On the telephone conversation with the Russian President, the European Commission President *"expressed concern at the gathering of Russian troops near the Ukrainian border, as well as the continuing flow of arms, equipment and militants from Russian territory"*[11], elements meant to aggravate the situation in Eastern Ukraine, not to help stabilise it. In this context, President Barroso *"warned against any unilateral military actions in Ukraine, under any pretext, including humanitarian"*[12]. Also, President Barroso asked Putin for help, using his influence to facilitate smooth and safe departure of civilians from areas controlled by pro-Russian separatists.

On 14 August, President Barroso spoke again on the phone with President Vladimir Putin about the situation in Ukraine. They discussed about ways that could contribute to de-escalate the conflict and the organisation of consultations between the presidents of Russia, Ukraine and the European Commission on issues related to the implementation of the Association Agreement. In order to discuss in detail these important issues it was agreed to use diplomatic channels.

On 26 August 2014, at the meeting in Minsk, the EU was represented by Catherine Ashton, the EU High Representative, Karel De Gucht, Commissioner for Trade, and Gunter Oettinger, Commissioner for Energy. President Lukashenko, President Putin, President Poroshenko, President Nazerbayev and EU representatives took part in the discussions and they focused on economic issues and issues related to peace and security in Eastern Ukraine.

President Barroso was in a continuous telephone contact with President Poroshenko and President Putin discussing about the crisis in Ukraine, about the need to prevent the escalation of conflict and reiterating the necessity of solving the crisis through a political solution. In his view, the visit of President Poroshenko on 30 August 2014 in Brussels *"is an important symbol of the European Union's continuing support for Ukraine and our commitment to achieving a political, negotiated solution to the conflict, which respects Ukraine's sovereignty, independence and unity"*[13]. So, the Ukrainian President's visit was a proof of the recognition of the efforts made by the EU to peacefully settle the crisis in this country.

[11] Commission Européenne, *Ukraine: entretiens téléphoniques du président Barroso avec le président Porochenko et le président Poutine*, Brussels, 11 August 2014, see http://europa.eu/rapid/press-release_IP-14-921_fr.htm, retrieved on 18 February 2015.

[12] *Ibidem.*

[13] European Commission, Brussels, *Statement by President Barroso following his Meeting with President Poroshenko of Ukraine*, 30 August 2014, see http://europa.eu/rapid/press-release_STATEMENT-14-265_fr.htm, retrieved on 18 February 2015.

As the crisis worsened in Ukraine, the EU set harsher and harsher restrictions. Thus, at the request of the European Council, the European Commission and the EEAS presented, on 3 September, *"a set of enhanced measures related to access to capital markets, defence, dual use goods, and sensitive technologies. Additionally, a new list of individuals (subject to sanctions), including the new leadership in Donbass, the government of Crimea as well as Russian decision-makers and oligarchs was presented"*[14]. The President of the European Council, Herman Van Rompuy, and the President of the European Commission, José Manuel Barroso, considered that the new package of restrictive measures against Russia was regarded as an effective tool that *"will increase the effectiveness of the measures already in place. It will also reinforce the principle that EU sanctions are directed at promoting a change of course in Russia's actions in Ukraine"*[15]. In the EU officials view, the more severe restrictive measures are the more effective they will be, and the ultimate goal is to change the attitude of the Russian Federation in Ukraine so that the moderation of Russia's actions to slow down the crisis worsening.

The EU acted from the very onset of the crisis in Ukraine by supporting it by sending repeatedly the High Representative in office at the time, Catherine Ashton, in Kiev. The purpose of the visits was the support offered to Ukraine to overcome the difficult situation it was going through. Catherine Ashton held talks with President Yanukovych and opposition leaders, on the one hand, and with the civil society representatives, on the other hand. Through her work, Catherine Ashton supported the conduct of presidential democratic elections and the formation of a new government in the same democratic spirit. The purpose of the EU HR Catherine Ashton's diplomatic efforts was to facilitate dialogue between the parties. There were also meetings of EU foreign ministers and meetings of Heads of State and Government on whose agenda was the evolution of the crisis in Ukraine. Among the top officials of the EU, both José Manuel Durão Barroso and Catherine Ashton reiterated the EU's desire that the crisis should be resolved peacefully through a political solution.

In addition to the mediation activities carried out, a notable achievement in the process of supporting Ukraine during the mandate of the EU HR Catherine Ashton was the Association Agreement between the EU and Ukraine signed on 27 June 2014.

[14] European Council, *Joint Letter to the EU Heads of State or Government by the President of the European Council, Herman Van Rompuy, and the President of the European Commission, José Manuel Barroso, on Restrictive Measures against Russia*, Brussels, 5 September 2014, see http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/144670.pdf, retrieved on 20 February 2015.

[15] *Ibidem.*

In November 2014, once concluded the mandate of the EU HR Baroness Catherine Ashton, Federica Mogherini was appointed. She continued the diplomatic activities started by the former head of European diplomacy. In this respect, Federica Mogherini travelled to Kiev on 16 and 17 December, where she attended meetings with the President of Ukraine Petro Poroshenko, the Prime Minister Arseniy Yatsenyuk and the Ukrainian Government, representatives of the opposition and civil society. Following the meetings, the newly appointed EU HR declared that *"The EU stays firmly and strongly at the side of Ukrainian people (…) to support the process initiated in Minsk to implement all the points that are in the Minsk agreement"*[16]. With this statement, it is reaffirmed the EU position to support Ukraine and to promote a peaceful solution to solve a violent conflict.

With the intensification of violence in Eastern Ukraine, in February 2015, the EU HR expressed concern about the continuous development of the crisis: *"The fighting provoked by the continued separatist offensive, notably around Debaltseve, is causing great human suffering and undermines all efforts aimed at a political solution"*[17]. According to Federica Mogherini, the only solution for peace in Ukraine is to respect the ceasefire agreement, and this is one of the EU priorities; another priority is to provide financial support to OSCE: *"The Minsk agreements must be fully implemented, this is our common priority. The EU is already providing substantial practical and financial support to the OSCE mission. We are now working to increase our support to OSCE so that it can fully play its role on the ground"*[18]. Despite the worsening situation in Ukraine, on 6 March 2015, Federica Mogherini maintained her position relating to a peaceful, political settlement of the crisis and not a military solution.

The Minsk Agreement signed on 12 February 2015 – Minsk II, due to the diplomatic mediation efforts of the French President, François Hollande, and the German Chancellor, Angela Merkel, on the negotiations between the Russian President, Vladimir Putin, and the Ukrainian President, Petro Poroshenko, was perceived as a success for the European diplomacy. At the same time, the observance of the agreement was regarded with distrust in what concerns the attitude of pro-Russian separatists. Indeed, the ceasefire agreed upon in Minsk II entered into force on 15 February, but it was violated by pro-Russian rebels,

[16] European Union External Action, *EU High Representative Visits Ukraine*, 17/12/2014, see http://eeas.europa.eu/top_stories/2014/171214_hrvp_visits_ukraine_en.htm, retrieved on 21 February 2015.

[17] European Union External Action, *Statement by High Representative/Vice-President Federica Mogherini on the Latest Development in Eastern Ukraine*, Brussels, 04/02/2015, see http://eeas.europa.eu/statements-eeas/2015/150204_01_en.htm, retrieved on 24 February 2015.

[18] European Union External Action, Press Realease, *Call between the HR/VP Federica Mogherini and UN Secretary General Ban Ki-moon on the Situation in Ukraine*, 24.02.2015, see http://eeas.europa.eu/statements-eeas/2015/150224_02_en.htm, retrieved on 24 March 2015.

who continued the offensive and managed to impose their control over the city of Debaltseve. Although Minsk II was not observed, despite repeated calls by EU officials, it was an important step towards a lasting political solution to end the crisis in Ukraine.

The EU has stepped up its efforts to assist Ukraine, so, on 22 July 2014, the Council set up the EU Advisory Mission for Civilian Security Sector Reform in Ukraine (Ukraine EUAM), a civilian mission launched on 1 December 2014. The objectives of EU advisors are initially aimed at supporting the development of revised security strategies and rapid implementation of reforms, in coordination with other actions of the EU, OSCE and other international partners[19]. The EU Advisory Mission for the Civilian Security Sector Reform in Ukraine aims at providing strategic advice for the development of sustainable and efficient security services that contribute to strengthening the rule of law in Ukraine[20]. In this respect, the EUAM Ukraine initiated a series of actions that included, *inter alia*, monthly discussion panels on various topics with the support of advisors in the mission, finding ways to improve the penitentiary legislation and its reform in cooperation with the Ukrainian authorities, the launching of a forum – the *Border Management Assistance Group (BMAG)* – to identify, analyse and solve border management problems in Ukraine with the Ukrainian authorities and international organisations interested in cooperation in this field.

Supporting OSCE mission in Ukraine by the EU is part of the continued EU actions to support Ukraine. In this context, the EU has provided approximately two thirds of the budget and most of the mission observers. On 23 May 2014 the EU decided to allocate 10 million EUR in support of the OSCE mission in Ukraine to enhance public confidence in preparing and organising the presidential elections on 25 May. This financial aid from the EU enabled the OSCE to deploy 105 additional election observers from the EU and the maximum number of 500 international observers, thus contributing to reducing tensions and fostering peace, stability and security in the entire Ukraine[21]. Also, on 6 April 2015, the EU donated 40 unarmoured vehicles and 24 armoured vehicles[22] to further support the efforts of the OSCE mission in Ukraine.

[19] Council of the European Union, *EU Establishes Mission to Advise on Civilian Security Sector Reform in Ukraine*, Brussels, 22 July 2014, see http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/144079.pdf, retrieved on 19 May 2015.

[20] European Union External Action, *EUAM Ukraine*, see http://www.eeas.europa.eu/csdp/missions-and-operations/euam-ukraine/index_en.htm, retrieved on 19 May 2015.

[21] *Increased EU Support for the OSCE's Work in Ukraine*, Brussels, 23 May 2014, see http://eeas.europa.eu/statements/docs/2014/140523_03_en.pdf, retrieved on 19 May 2015.

[22] European Union External Action, *EU Donates Vehicles to the OSCE Special Monitoring Mission (SMM) to Ukraine*, see http://eeas.europa.eu/csdp/missions-and-operations/euam-ukraine/news/20150311_en.htm, retrieved on 20 May 2015.

The main feature of the EU action in the conflict in Ukraine in the field of common foreign and security policy is the comprehensive approach, reflected by diplomatic means, political, economic, financial measures and the deployment of a civilian mission, all of which contributing to unwinding conflict which has caused more than 6,000 casualties so far.

Conclusions

The first measures adopted by the European Union in order to determine a more cooperative attitude from the Russian Federation to prevent conflict escalation were restrictive measures and, gradually, economic and diplomatic sanctions.

The restrictive measures imposed by the European Union on those who have contributed to the impaired integrity and sovereignty of Ukraine are of gradual evolution. Thus, initially, there were implemented restrictive measures for a limited number of people associated with actions against the territorial integrity of Ukraine who were banned from entering the EU and whose assets were frozen. Gradually, restrictive measures have been extended to some Russian companies. To increase the effectiveness of the restrictive measures in force, economic sanctions and then diplomatic measures against the Russian Federation were also applied. The restrictive measures became more stringent, restricting, for instance, Russia's access to capital markets in the EU. The restrictions focused on defence area, sensitive technologies or energy. Moreover, the European Union imposed sanctions targeting Crimea and Sevastopol. Thus, by prohibiting goods imports in these areas and by subsequently introducing significant additional sanctions on investments, services and trade with Crimea and Sevastopol, the EU has given a clear signal that it does not recognise their annexation by Russia.

On 28 November 2014, 132 people were under the EU sanctions, because of their involvement in activities detrimental to the territorial integrity of Ukraine and the assets of 28 entities were frozen by the EU[23], their number increasing as the situation in Ukraine continued to worsen.

Mediation and dialogue were, are and will be the main tools used by the European diplomacy. With the establishment of the position of High Representative of the Union for Foreign Affairs and Security Policy and the European External Action Service, the EU diplomacy has become more coherent and effective.

One month after taking office of High Representative, Catherine Ashton made known her work objectives and the EU aspiration to raise the importance

[23] Conseil de l'Union européenne, *L'UE renforce les sanctions à l'encontre des séparatistes opérant dans l'est de l'Ukraine*, Brussels, 28 November 2014, see http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/FR/foraff/145968.pdf, retrieved on 21 February 2015.

of its political action by discreet diplomacy and concerted action. The Head of European diplomacy considered that: *"It is important for the EU to pursue an active role in areas affected by crises and conflicts. It is the responsibility of a <global player>, as well as an integral part of a security policy for Europe"*[24]. The EU efforts to resolve the crisis in Ukraine go this way.

The diplomatic activity of both Catherine Ashton and her successor, Federica Mogherini, to solve the crisis in Ukraine has resulted in sustained efforts to support the implementation of a political solution through mediation and facilitation of a peaceful dialogue between the parties.

Catherine Ashton considers that the EU efforts to help maintain international peace and security are based on three pillars; *"the direct involvement in the international negotiations on behalf of the international community; the ability to implement a comprehensive approach and use a wide range of tools to solve crises, and the close work with the international and regional partners, where only collective efforts can deliver results"*[25].

Regarding the crisis in Ukraine, by diplomatic efforts, the European Union has significantly contributed to the efficiency of the international diplomacy in solving the crisis in this country. Unfortunately, despite the reactions of the international community to condemn the armed aggression perpetrated in Ukraine, the sanctions imposed on Russia, the intense international diplomatic efforts, the crisis has continuously evolved and its settlement will be a long process whose end, at least in the near future, cannot be predicted and will require the international community intense diplomatic efforts.

[24] Catherine Ashton, *Diplomazia discreta e azione concertata* in *La Stampa*, 22/12/2009, see http://www.lastampa.it/2009/12/22/cultura/opinioni/editoriali/diplomazia-discreta-e-azione-concertata-VLSeTEfzj0jWDxC7xqb6eK/pagina.html, retrieved on 16 February 2015.

[25] Nations Unies, *Le Conseil de sécurité salue « l'importante contribution » de l'Union européenne au maintien de la paix et de la sécurité internationales*, 14 February 2014, see http://www.un.org/press/fr/2014/CS11279.doc.htm, retrieved on 22 February 2015.

CROSS-CUTTING SECURITY CHALLENGES IN ROMANIA'S VICINITY

Dr Cristina BOGZEANU

Romania has been often considered a "victim" of geopolitics, its geographical location exposing it to various risks and threats in the course of its entire history. Recent events show that, despite the security guarantees achieved as NATO and EU member state, Romania is still placed in an arc of instability, giving rise to considerable security challenges.

The premise of the present study is that, although the escalation of the Ukrainian crisis fully justifies the extent to which the attention and resources are directed in this sense, instability in Western Balkan space should not be underestimated and, so much the less, omitted.

***Keywords**: Western Balkans; Wider Black Sea Area; Russian Federation; Ukrainian crisis; security*

1. Romania under the East-European Arc of Instability

Both the academic and political approaches to the current political and military crisis in Ukraine have been built on two major directions. The first one, most frequently used and materialised in the numerous economic sanctions imposed on Russia, consists in the condemnation of the Russian Federation's actions in Ukraine, considered grave violations of international law principles. Another interpretation, not as famous as the previous one, but with a considerable impact, is based on the idea that Moscow's actions in Ukraine were determined, fostered, provoked, to a certain extent, by Western actors[1]. The Ukrainian crisis, which had its first phases in late 2013, was the result of the overlapping interests

Dr Cristina Bogzeanu – researcher within the Centre for Defence and Security Strategic Studies, *"Carol I"* National Defence University, Bucureşti.

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

[1] John J. Mearsheimer, *Why the Ukraine Crisis is the West's Fault. The Liberal Delusion that Provoked Putin*, in *Foreign Affairs*, September/October 2014, see http://www.foreignaffairs.com/articles/ 141769/ john-j-mearsheimer/why-the-ukraine-crisis-is-the-wests-fault, retrieved on 15 November 2014.

of the Kremlin, on the one hand, with the ones of the Western actors, on the other hand, especially NATO and the EU.

The conclusions are questionless and unanimously accepted – recent events represent the most notable challenge to Europe's security since the end of the *Cold War*. Russia's aggression[2] in Ukraine has brought again *"the spectrum of war"* in Europe. Undoubtedly, there is also a veritable diplomatic crisis between the Western actors (namely, the USA, NATO, and the EU) and the Russian Federation; cooperation between these parties has been considerably reduced, with a difficult and tensed dialogue and a slow negotiation process, all these aspects being marked by the economic sanctions imposed by Occidental actors on Russia and by the maintenance of a negative rhetoric of the Russian Federation regarding NATO and EU actions, especially those concerning their enlargement, the efforts to consolidate partnerships with former Soviet states, and the deployment of the Alliance's military capabilities on the territory of the states near Russian borders.

The extent of the consequences of both the Ukrainian crisis and the diplomatic crisis between the West and the Russian Federation were emphasised by the German Chancellor during a speech held at Lowry Institute for International Policy (Sydney, 17 November 2014): *"This isn't just about Ukraine. This is about Moldova, this is about Georgia, and if this continues then one will have to ask about Serbia and one will have to ask about the countries of the Western Balkans"*[3].

[2] Officially, the Russian Federation denied on repeated occasions its military involvement in the conflict in Eastern Ukraine. However, Western actors' official declarations and positions clearly reveal the existence of obvious proofs that the reality is entirely different. For instance, the text of the Wales Summit Declaration includes references to Russian aggressive actions in Ukraine: *"We condemn in the strongest terms Russia's escalating and illegal military intervention in Ukraine (...). We demand that Russia (...) refrain from aggressive actions against Ukraine (...). We are extremely concerned by the further escalation of aggressive actions in Eastern Ukraine. We see a concerted campaign of violence by Russia and Russian-backed separatists aimed at destabilising Ukraine as a sovereign state"*. For details, see *Wales Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales*, 24 September 2014, http://www.nato.int/cps/en/natohq/official_texts_112964.htm, retrieved on 8 June 2015. Also, for detailed information on Russia denying its military involvement in Ukraine and on proofs revealing the opposite, see Maksymilian Czuperski, John Herbst, Eliot Higgins, Alina Polyakova, Damon Wilson, *Hiding in Plain Sight. Putin's War in Ukraine*, Atlantic Council, Washington D.C., May 2015, see http://www.atlanticcouncil.org/publications/reports/hiding-in-plain-sight-putin-s-war-in-ukraine-and-boris-nemtsov-s-putin-war?gclid=CKDGpMuDgsYCFY7MtAodV3AAQQ, retrieved on 8 June 2015.

[3] Roland Oliphant, *Angela Merkel Warns Russia Could Seek to Destabilize Whole of the European Peace and Order*, *The Telegraph*, 17 November 2014, see http://www.telegraph.co.uk/news/worldnews/europe/germany/angela-merkel/11236622/Angela-Merkel-warns-Russia-could-seek-to-destabilise-whole-of-the-European-peaceful-order.html, retrieved on 1 April 2015.

Within the present paper, cross-cutting security challenges will be considered those security trends characteristic to Romania's vicinity, similar in their nature or reinforcing each other, and influencing Romania's national security. These trends do not directly regard Romania and are not necessarily characteristic to it, but, through the instability they trigger, cross-cutting security challenges determine the undertaking of a set of measures with a view to managing their effects.

The possibility of a connection between the crisis from the Black Sea area and the Western Balkans destabilisation can be considered an overstatement, an overbid of the Ukraine crisis' potential to reverberate on the European security environment. Nonetheless, the common aspects characteristic to these two spaces fully justify considering this possibility. The two regions are similar in their structural instability (fragile states, poor economic and democratic development etc.), their long history of conflicts, as well as their value of strategically important areas, especially in the energy domain, as they are transit zones for Russian and Central Asian hydrocarbons to Central and Western Europe. Subsequently, it is not a coincidence that both the Wider Black Sea Region (WBSR) and the Western Balkan states have attracted great regional powers' interest, each of them trying to gain more influence than the other.

For Romania, NATO and EU border state, the context is considered to be even more challenging, given its 600 kilometres of common border with Ukraine. However, from our perspective, Romania's current security challenges are not concentrated exclusively in its Eastern vicinity, but also in its South-Eastern neighbourhood. Since the end of the violent disintegration of Yugoslavia, the Western Balkans' security dynamic has been characterised by a certain improvement in stability, but the formation of stable or relatively stable states in this area is still a desideratum to be achieved.

Romania's geographical location as vulnerability has been emphasised in numerous geopolitical studies. During its entire history, being a Black Sea riparian state has meant being in a space disputed between great powers, with the potential of becoming the arena of open military confrontations.

The Black Sea's weight in Russian and Romanian geopolitical calculi, as well as this region's destabilising potential has also been approached by the famous Romanian historian and politician, Gheorghe I. Brătianu, who, during a course held at the University of Bucureşti (1941-1942), *The Black Sea Question*, mentioned the existence of two key positions in the Black Sea, which Romania had to include in its geostrategic calculi: a) Bosporus entrance and b) Crimea that, *"by its natural harbours, its strongholds from ancient times, by the fact that it represents a maritime bastion in the Black Sea has obviously a master* *position over the entire maritime complex in the region. The one who has Crimea can control the Black Sea. The one who does not have it cannot control it"*[4].

In a much more recent paper, speaking about Mackinder's vision of Eastern European states, the Romanian sociologist and geopolitician, Ilie Bădescu, describes the Ponto-Baltic isthmus as a buffer space between the Eurasian power and the European one, underlining the importance of maintaining the independence of the states in this area for the European security. In the view of the Romanian geopolitician, Eastern European states represent *"the little geopolitical strokes that can fell the great geopolitical oaks of great states"*[5].

Romania's location in the Western Balkans' vicinity is also full of importance. Political-military crises in this area are already in their de-escalation phases, the actors involved being in course of post conflict stabilisation and reconstruction. Nonetheless, this region's potential of being the scene of new crises and a new escalation of current crises are considerable, especially in the case of Kosovo and Bosnia and Herzegovina. The fact that Russia plays a major role both in the WBSR and Western Balkans' geopolitics adds concern to the above-mentioned aspects.

Also, one should not underestimate the destabilising potential of this region, whose stability is still challenged by the multitude of ethnic groups and religions, the populations still showing strong feelings of hostility to each other, which sporadically results in street fights. The maintenance of peacekeeping missions in Kosovo is relevant in this respect. Moreover, besides inter-ethnic tensions, the Western Balkans pose security challenges to which there have not been found consistent political solutions yet.

From a geopolitical point of view, Romania is placed in a unique context, at least at this region level. It is the sole NATO and EU border state directly neighbouring two spaces with a major destabilising potential, which are extremely vulnerable in terms of internal political, social and economic organisation, as well as regarding external influence. Additionally, Romania's Eastern and South-Western neighbourhoods are subject to external pressures, especially considering the clearly antagonistic interests and positions expressed by Moscow and Western actors (the USA, NATO and the EU) in the context of the Ukraine crisis.

[4] ***, *Viaţa şi activitatea lui Gheorghe I. Brătianu*, Asociaţia Europeană de Studii Geopolitice şi Geostrategice *"Gheorghe I. Brătianu"*, see http://www.aesgs.ro/page.php?id=8&s1=67, retrieved on 16 December 2014.

[5] Ilie Bădescu, *Geopolitica Heartlandului Eurasiatic. Rusia: o perspectivă non-ideologică*, in Ilie Bădescu, Lucian Dumitrescu, Veronica Dumitraşcu, *Geopolitica noului imperialism*, Editura Mica Valahie, Bucureşti, 2010, pp. 287-288.

The difference between becoming a bridge of stability, with a major function in conveying stability and security towards both South-West and North-East, and becoming a bridge of instability will be given by the manner in which Romania will make the most of its extremely advantageous geopolitical location, although it is not void of difficulties, as well as by the manner in which it will assume its vulnerabilities, weaknesses, which can impinge on its capacity of coping with the consequences of political-military crises in the Western Balkans and the WBSR.

2. Factors of Destabilisation in the Western Balkans and their Relevance in the Context of the Ukraine Crisis

2.1. Serbia

Although they share a deeply conflictual history, the two spaces under discussion manifest differences from certain points of view. Thus, the space adjacent to the Black Sea is under a clear economic, political, military and even social Russian influence. Traditionally considered a Russian sphere of influence, even after the end of the *Cold War*, this space has been under its ascendant, kept not only by making use of economic blackmail (especially in the energy area), but also by maintaining and feeding frozen conflicts, keeping the states in this region in a continuous state of instability. Certainly, the physical closeness to the Euro-Atlantic space has also determined cooperation initiatives of the Western actors, so that the actors in this area have been included in various formats of cooperation with NATO and the EU. The Union has mainly focused on economic cooperation, launching initiatives such as the Eastern Partnership, while cooperation with NATO has been developed within the Partnership for Peace. However, any attempt of the West to increase, enhance or deepen cooperation with WBSR states was followed by harsh reactions of Moscow. In this line of thought, it is not a coincidence that the war in Georgia (2008) took place after the Allies opened the perspective of membership for Kiev and Tbilisi during the Summit in București and while the EU was preparing to launch the Eastern Partnership.

In the Western Balkans prevails the Occidental influence. Even though the actors in this region are still far away from being characterised as self-governable and stable states, NATO and EU presence and influence have certainly had a positive impact in terms of the region stabilisation and the development of a culture of cooperation between these states after the end of the Yugoslav wars. Even more, unlike WBSR states, where the relations with the two organisations are carried out within a series of partnerships, in the case of Western Balkans states, there is a clear chance to become NATO and EU member states. Their efforts to meet the accession standards have constituted the main stimuli for their economic, political, and military development and modernisation.

The conflictual atmosphere is kept by a mix of factors reinforcing each other, giving rise to a vicious circle of instability: interethnic tensions, economic difficulties reflecting in a low level of the citizens' quality of life, lack of cohesion at the level of political class, corruption etc.[6].

However, the Western Balkans gain greater significance in the context of the events in Ukraine as they attract the interests of both the West and the Russian Federation. If NATO and EU roles are obvious, Russian interests are not as visible as theirs or as the interests in the WBSR. *"If EU enlargement to the East has served to safeguard Europe's Eastern flank, the focus should now be on the countries stuck in the middle. At a time when geopolitics is back on the agenda, the situation of the Balkans should return to the limelight. Despite being at some distance from the hotspot, their poor economic situation and their remaining unresolved conflicts make them the weakest part of Europe"*[7].

One of the most sensitive aspects in this regard is the relation between Russia and Serbia, the latter expressing, under the conditions of the Ukrainian crisis, its neutrality, refusing to rally to the economic sanctions and bans imposed by the EU to Moscow, in spite of being an EU candidate country. For justifying its position on this issue, Belgrade invoked the national interests, especially the energy dependency on Russia. But, the fact that other Western Balkan states, also on their way of becoming EU member states and also dependent on Russian energy resources, rallied to the sanctions imposed on Russia reveal that this type of motivation does not entirely justify Belgrade's attitude in this context.

Serbia is often defined as a Moscow's traditional ally due to a common cultural background. Russian-Serbian relations have recently known a phase of consolidation and enlargement. In May 2013, Moscow and Belgrade signed a strategic partnership, in November 2013, a bilateral agreement on military cooperation and, in April 2013, Serbia became a *CSTO (Collective Security Treaty Organisation)*[8] observer.

[6] This state of facts is visible in the evolutions of these states in *Failed/Fragile States Index*, see http://library.fundforpeace.org/library/cfsir1423-fragilestatesindex2014-06d.pdf, retrieved on 21 January 2015.

[7] Raquel Montes Torralba, *Belgrade at the Crossroads: Serbian-Russian Relations in Light of the Ukraine Crisis*, Elcano Royal Institute, Análisis del Real Instituto Elcano, no. 63/2014, 22 December 2014, see http://www.realinstituto elcano.org/wps/portal/web/rielcano_en/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_in/zonas_in/ari63-2014-montes-belgrade-crossroads-serbian-russian-relations-ukraine-crisis#.VTPbpSHBzRY, retrieved on 12 April 2015.

[8] CSTO was established in 1992 as a political-military organisation, being composed of six member states: Russia, Armenia, Belarus, Kazakhstan, Kirghizstan, and Tajikistan.

In this respect, it would be useful to recall that, during the war that ended with the disintegration of Yugoslavia, Serbia was one of NATO's bombing targets. Since then, Belgrade has cooperated with the Alliance in numerous aspects related to the security and defence sector reform, the most important cooperation area being KFOR contribution to maintaining security in the province of Kosovo. Nevertheless, unlike all the other Western Balkan states, Serbia is the sole actor that has not included the membership of NATO among its main foreign policy objectives. Even more, through the *resolution on the protection of sovereignty, territorial integrity and constitutional order of the Republic of Serbia*[9], Belgrade declares its military neutrality, which is translated in the exclusion of the objective of being fully integrated into the Alliance, but without meaning that it has completely renounced NATO cooperation. Moreover, the relations between Serbia and NATO have known a cooling period in 2008-2010, due to the Alliance's support for Kosovo's independence. Also, the project of joining the Alliance does not have the population support, being rejected by 7 out of 10 Serbs[10], indicating that NATO's bombings in the '90s are still widely present in the Serb population's memory.

Besides the Christian-Orthodox common culture, frequently invoked as a fundament of Russian-Serbian relations, their recent history has also been marked by the support offered by Moscow to Belgrade regarding Kosovo's declaration of independence, especially as the Kremlin could express its opposition in this respect within the UN Security Council. Russia's attitude has turned out to be ambivalent, taking advantage of the issue of this province's separation in its own interest. If, in 2008, Russia used its veto right in the UN Security Council regarding Kosovo's independence, during the same year, it stood on the fact that most EU and NATO member states recognised the independence of the Serbian province in order to justify the legitimacy of the independence of the two Georgian separatist republics – Abkhazia and South Ossetia. Even more, the recognition of Kosovo by the West was also invoked by V. Putin as a precedent in his already famous speech on 18 March 2014*: "a precedent our Western colleagues created with their own hands in a very similar situation"*[11]. Within the same speech, Putin also referred to a Written Statement of the USA according to which, although the acts of independence can be a violation of the internal legislation, they are not necessarily a violation

[9] ***, *Serbian Parliament's Kosovo Resolution*, 27 December 2007, see http://www.b92.net/eng/insight/ strategies.php?yyyy=2007&mm=12& nav_id=46517, retrieved on 4 October 2014.

[10] ***, *Serbia's Stance on NATO and the EU*, in *Stratfor Analysis*, 2 August 2012, see https://www.stratfor.com/analysis/serbias-stance-nato-and-eu, retrieved on 3 September 2014.

[11] ***, *Full Text of Putin's Speech on Crimea*, in *Prague Post*, 19 March 2014, see http://praguepost.com/eu-news/37854-full-text-of-putin-s-speech-on-crimea, retrieved on 12 February 2015.

of the international law, emphasising that this is exactly what the Russians, Ukrainians and Tatars from Crimea had done[12].

Also significant is the consolidation of the Russian-Serbian relations in the context of the Ukraine crisis; even more, it is not the first time when Moscow adopts such a strategy. Immediately after NATO Summit in Bucureşti (2008), when the Allies opened the possibility for the integration of Ukraine and Georgia, followed by the war in Georgia (2008), in 2009, the Serbian minister of interior and the Russian minister for emergency situations signed an agreement for the creation of a centre for humanitarian emergencies at Nis, until 2012. Located at a distance of 200 kilometres from Romania and close to Kosovo province, Nis is known for being an important military centre within both Yugoslavia and Serbia[13]. This is the reason lying at the basis of the suppositions that Nis humanitarian centre could evolve towards a military base[14].

From an economic point of view, Russian-Serbian relations are far away from playing a significant role in Serbia's economic life. Thus, although Russia's economic presence, mainly concentrated in Serbia and in Bosnia and Herzegovina (especially in Srpska Republic), is the greatest since 1990 until present, the *Economist Intelligence Unit* shows that, in 2013, only 8.5% of Serbia's trade relations were directed to Russia, while the EU accounted for 62.4% of its trade[15].

However, the relations between these actors in the energy sector are of great significance. The Western Balkans are a space of major interest not only because of these states' dependency on the imports of Russian hydrocarbons, but also as a transit route for the Russian energy resources (especially natural gas) to Central Europe. *South Stream* Project is an eloquent example in this respect. The project was considered one of the main alternatives for continuing the natural gas export to the centre of Europe, letting Ukraine aside, as well as an alternative for the EU's *Nabucco* project. The fact that on 1 December 2014, the Russian President announced South Stream's cancellation is a token of a new escalation of the tensions between Moscow and the West.

[12] *Ibidem.*

[13] ***, *Serbia: Russia's Eyes on the Balkans*, in *Stratfor Geopolitical Diary*, 21 October 2009, see https://www.stratfor.com/geopolitical-diary/serbia-russias-eyes-balkans, retrieved on 10 April 2015.

[14] ***, *Russia's Opportunity in Serbia*, in *Stratfor*, 6 May 2011, see https://www.stratfor.com/analysis/russias-opportunity-serbia, retrieved on 10 April 2015.

[15] ***, *Russia in the Balkans*. Conference Report, The Balkans in Russia's Foreign Policy Strategy, Russia and Conflict Resolution in the Balkans, The Economic Dimension, London School of Economics Research on South-Eastern Europe & South East European Studies at Oxford, 13 March 2015, see http://www.lse.ac.uk/european Institute/research/LSEE/Events/2014-2015/Russia-in-the-Balkans/merged-document.pdf, pp. 8-9, retrieved on 15 April 2015.

Besides all these aspects, there are also Moscow's massive investments in Serbia's railways (about 750 million EUR), the fact that Lukoil holds 79.5% of the local petrol station network – Beopetrol, and Gazprom is the main stakeholder in the country's greatest natural gas provider. Actually, by this strategy, Russia counterbalances NATO and US strategic influence in this area. Thus, Russian energy companies control to a great extent modern refinement *complexes, networks of petrol stations and oil and gas transport, making the Balkan economies highly dependent on Russia in this domain*[16].

2.2. Separatism and extremism in Bosnia and Herzegovina

Another leverage by which Russia exerts its influence in the Western Balkans is connected to the Srpska Republic. This is one of the two entities composing Bosnia and Herzegovina, inhabited preponderantly by a population of Serbian ethnics, which has constantly manifested, at political level, the tendency and the wish to separate from Bosnia and Herzegovina and to unite with Serbia. This desideratum has remained out of discussions mainly due to Kosovo issue and to the obvious parallelism that could be made in this respect. However, the Srpska Republic could be a good environment for Russia to capitalise on its soft power, by appealing to the common Christian-Orthodox cultural background, similarly to the situation of Serbia.

Bosnia and Herzegovina population is strongly divided along ethnic lines[17], which contributes to this country's political and economic instability. Political stalemate is a constant in Bosnia and Herzegovina's internal life, turning into an obstacle towards making economic and social progresses. Similarly to the other Western Balkan actors, Bosnia and Herzegovina is clearly on its path to the Euro-Atlantic integration, but not without experiencing serious challenges in this respect. Of course, firstly, there are the inter-ethnic tensions, the difficult reform process and the slow pace at which political, economic, social, juridical and military reforms are made. But, in this case too, there can be identified a certain role played by the Russian Federation. The leader of the Srpska Republic, Milodrad Dodik, has been a constant supporter of the autonomy of this entity from Bosnia and Herzegovina, having, at the same time, solid relations with the Kremlin.

[16] Vasile Leca, *'Independenţa' Crimeei şi implicaţiile asupra zonei Mării Negre şi Balcani*, in *Revista 22*, 19 March 2014, see http://www.revista22.ro/ independenta-crimeei-si-implicatiile-asupra-zonei-marii-negre-si-balcani-39469.html, retrieved on 25 March 2014.

[17] According to CIA World Factbook, Bosnia and Herzegovina population is composed of 48.4% Bosniaks, 32.7% Serbs, 14.6% Croats, see https://www.cia.gov/library/publications/the-world-factbook/geos/bk.html, retrieved on 12 April 2015. Also, Srpska Republic is inhabited by a Serb majority, while the Federation of Bosnia-Herzergovina is mostly inhabited by Bosniaks and Croats.

Actually, the relation between Moscow and the Srpska Republic has been characterised as rather *"a relationship with another sovereign state and not with a semi-autonomous region inside Bosnia and Herzegovina"*[18].

The evolution of the Ukraine crisis, especially the annexation of Crimea, has fuelled the separatist rhetoric in the Srpska Republic. Even more, in November 2014, the Russian Federation abstained when the extension of EUFOR Althea mandate was discussed within the UN Security Council, due to the fact that the resolution referred to this country's prospects for the membership of the EU[19].

This attitude was considered a sign of the Kremlin's wish to keep Western Balkans states aside from the project of Euro-Atlantic integration, but one of the main conclusions drawn at the conference *"Russia in the Balkans"*, supported by NATO, reveals a distinct vision. Although it is clear that the Western Balkan region does not have the same importance for Russia as its close vicinity does, *"Russia is back to the Balkans in order to score points against the West by exploiting loopholes and blind spots in its policy (…), the overarching goal is not to roll back NATO and EU enlargement but to build influence in countries that are either part of Western clubs, or are well on their way to joining them, and are therefore useful door openers"*[20]. There is not unanimity of opinions in this respect as, according to other sources, the Kremlin's interest is to exert such a great pressure in the Balkans so as either to draw back those states from the Euro-Atlantic integration, or to be able to influence the EU's resolutions in favour of Russia, once they will have become EU member states[21].

Irrespective of the fact that Russia aims to counterbalance Western influence in the Western Balkans, in the same manner the West counterbalances its influence in its close vicinity, or that it aims to achieve a leverage of influencing the decisions taken at the European level or that it simply aims to increase its influence over a space with a major geostrategic significance, Moscow's actions in the Western Balkans have the potential to destabilise this region. This is even more evident under the conditions of the Ukraine crisis. In this context, the fact that Serbia took,

[18] Luke Coffey, *The US Must Counter Russian Influence in the Balkans, Issue Brief on Russia and Eurasia*, no. 4316, The Heritage Foundation, 9 December 2014, see http://www.heritage.org/research/reports/2014/12/the-us-must-counter-russian-influence-in-the-balkans, retrieved on 15 April 2015.

[19] Security Council, Resolution 2183 (2014), *Renews European Union-led Multinational Stabilization Force in Bosnia and Herzegovina for 12 Months*, 7307th Meeting (PM), 11 November 2014, see http://www.un.org/press/ en/2014/sc11641.doc.htm

[20] ***, *Russia in the Balkans…*, *op. cit.*, p. 2.

[21] Nikolaus Blome, Susanne Koelbl, Peter Müller, Ralf Neukirch, Matthias Schepp and Gerald Traufetter, *Putin's Reach: Merkel Concerned about Russian Influence in the Balkans*, in *Der Spiegel*, 17 November 2014, see http://www.spiegel.de/international/europe/germany-worried-about-russian-influence-in-the-balkans-a-1003427.html, retrieved on 2 April 2015.

at the beginning of 2015, OSCE presidency, with a major role in providing solutions for the conflict in Ukraine, is not void of significance.

Additionally, there is also a wide range of factors contributing to the destabilisation of the Western Balkans, which are not necessarily connected to Russia's strategy in the region, but rather to the increase in the frequency of the discourses referring to the autonomy and independence of some provinces and regions from the states in this space and to their unification with other states. We have already mentioned the case of the Srpska Republic, but, also significant is the declaration of the Albanian Prime Minister that the unification of Kosovo with Albania is unavoidable and undisputable. The declaration was harshly criticised by both the EU and Serbia, warning that the Albanian leaders should cease destabilising the region[22].

Another aspect gaining increasingly more weight in the dynamic of Western-Balkan security is related to the Islamic radicalisation, Kosovo and Bosnia and Herzegovina being the main subject in this respect. Both of them have populations with Muslim majorities (40% in Bosnia and Herzegovina, respectively, 95.6% in Kosovo[23]). Even more, 70% of the Kosovars are young people under 35, and the unemployment rate is extremely high (over 30%). In Bosnia and Herzegovina too unemployment has reached an alarming record – 44.3% in 2013[24]. As a consequence, these states have the potential of being a favourable environment for recruiting young men within extremist networks.

As far as Bosnia and Herzegovina is concerned, the majority of the Muslim population is moderate, but the Islamic community is increasingly asserting itself on the political scene, assuming leadership role in channelling population's frustrations and anger and filling the void of power left by the other political parties[25]. There have also been identified cases when combatants from Bosnia and Herzegovina joined extremist fighters in Syria and Iraq, as well as cases of recruitment and financing Bosnians for joining Islamist militants in these countries[26].

Kosovo was the scene of similar events, the authorities estimating that, in August 2014, between 100 and 200 Kosovar Albanians were involved

[22] Andrew Rettman and Ekrem Krasniqi, *EU Says Albania Comment on Kosovo Unification Not Acceptable*, in *EU Observer*, 9 April 2015, see https://euobserver.com/foreign/128273, retrieved on 9 April 2015.

[23] CIA World Factbook, see https://www.cia.gov/library/publications/the-world-factbook/, retrieved on 10 April 2015.

[24] *Ibidem.*

[25] ***, *Bosnia's Dangerous Tango: Islam and Nationalism*, Europe Briefing No. 70, International Crisis Group, 26 February 2013, see http://www.crisis group.org/~/media/Files/europe/balkans/bosnia-herzeg ovina/b070-bosnias-dangerous-tango-islam-and-nationalism.pdf, retrieved on 25 April 2014.

[26] ***, *Bosnia Detains Suspected Jihadists*, RFE/RL's Balkan Service, 3 September 2014, see http://www.rferl.org/content/bosnia-detains-suspected-jihadists/26564672.html, retrieved on 3 September 2015.

in the conflicts in Syria and Iraq, on the side of extremist fighters. There were also arrested extremist leaders for trying to recruit young men in order to become Islamic combatants in the aforementioned countries.

Extremism's tendency to amplify, together with other security challenges specific to the region (organised crime), can constitute a genuine security risk at Europe's border and in Romania's immediate vicinity. It is also relevant in this respect that, in this region, there are still substantial armament stocks[27], despite the numerous international initiative carried out in order to reduce them.

Practically, in this area, the balance between the influence of the Western actors and the Russian Federation, the structural instability and the development of extremism have the potential for destabilising the region.

3. General Conclusions and Implications for Romania

The security environment in Romania's neighbourhood has become a very dynamic one, the source of numerous and diverse security challenges, with major impact on our country's national security. The repercussions are complex as the geographical area in which Romania is placed has been considered, especially since it became a NATO and EU member state, relatively stable and secure. Moreover, the two organisations have built a genuine network of partnerships with the states from our vicinity, which are not members. The European Neighbourhood Policy, the Eastern Partnership, the entire range of cooperation initiatives launched for this region, NATO Partnership for Peace are meant to increase the level of predictability of the security evolutions in this area, to contribute to the development of mutual trust between actors, to create the proper framework for the economic development etc. Even more, in the case of the Western Balkans, after the end of the violent confrontations having led to the disintegration of Yugoslavia, NATO and the EU have considered the possibility of these countries membership, seen as the solution that could put an end to the violent history of these actors and this region's conflict potential.

The recent period, marked by Russia's aggressive actions in Ukraine, by the territorial annexation of Crimea, by the emergence of a genuine diplomatic crisis between the East and the West, by the maintenance of a continuous aggressive rhetoric of Moscow towards NATO and EU actions in this space, clearly sets as a new stage of regional evolutions in this area.

[27] In 2011, the surplus of armament declared by Serbia, Albania, Bosnia and Herzegovina, Croatia and Montenegro amounted to 414,992. For details, see Pierre Gobinet, *Significant Surpluses: Weapons and Ammunition Stockpiles in South-East Europe*, Special Report, Small Arms Survey, Switzerland, December 2011, p. 26, http://www.smallarmssurvey.org/fileadmin/ docs/C-Special-reports/SAS-SR13-Significant-Surpluses.pdf, retrieved on 14 August 2014.

Ever since it joined NATO and the EU, Romania's national security has been thought almost exclusively in relation to its membership of Euro-Atlantic structures, which equals, beyond doubt, with the most consistent security guarantee Romania has ever benefited of in its entire history. Romania's neighbourhood is defined, as we have shown in the previous pages, by both an increased level of instability and its major strategic importance. One of the most relevant features of the geopolitics of this space resides in the confluence of interests and common vulnerabilities amplifying each other, altogether creating the image of cross-cutting security challenges.

The study of these crises' implications on Romania's security has to be founded on its status of NATO and EU member and border state. However, in the current international and regional security environment, it is necessary to relate to this status more beyond the security guarantees, attaching more importance to the assumed obligations and responsibilities. Also, this status places Romania without doubt on the Western actors' side in the context of the Ukraine crisis and the Western Balkans ones, despite the different position adopted in the Kosovo issue[28].

One of Romania's national interests is to assert itself as a relevant regional actor, with strategic significance for the Allies and for the organisations with security vocation to which it belongs[29], the added value that Bucureşti can bring within these organisations consisting in the approach to these cross-cutting security challenges. Subsequently, the manner in which Romania reacts in this context gains a major significance not only regarding the way in which it asserts on the international arena, but also for our country's level of security.

With a 600 kilometre long common border with Ukraine, with a special relation with the Republic of Moldova and with a relative dependency on Russian hydrocarbons' imports, Romania is one of the most vulnerable states to the increasing instability in Eastern and South-Eastern Europe.

Romania's complex situation at present is not given only by its position on Kosovo issue, but also by its special relation with the Republic of Moldova and its role in the management of Transnistria, another crisis with major implications

[28] Although most of Euro-Atlantic actors recognised Kosovo's independence, Romania is one of the five European states which has not rallied to this position. The motivation resides in the belief that such an act would encourage separatism in the region, and the recent security dynamic in the Wider Black Sea Region supports the legitimacy of Romania's argument in this respect. For details on Romania's motivation regarding its position on Kosovo's declaration of independence, see: *MFA statement regarding the Advisory Opinion on the "accordance with international law of the unilateral declaration of independence by the Provisional Institutions of Self-Government of Kosovo" of the International Court of Justice*, http://www.mae.ro/en/node/4168, retrieved on 10 April 2015.

[29] ***, *Romania's National Security Strategy*, Bucureşti, 2007, p. 18, see http://www.isn.ethz.ch/Digital-Library/Articles/Special-Feature/Detail/?lng=en&id=156800, retrieved on 20 April 2015.

on Romania's security and regional stability. In the context of the Ukrainian event, Transnistria's situation becomes even more difficult. Eloquent in this respect is the reiteration of the idea that Transnistria should be included within Russia's territory. The president of Transnistria's parliamentary assembly made such a request soon after the annexation of Crimea, but it was withdrawn within a short time. All these under the conditions in which the relations between Romania and Russia have not been extremely close in the recent history. Their different views regarding Transnistria's status and the Republic of Moldova's pathway, Romania's membership of Euro-Atlantic structures, Romania's hosting elements of US anti-missile shield, the perspectives on Southern Caucasus separatist republics, on Ukraine crisis or Romania's treasury are the main issues influencing this relation.

The escalation of the tensions between the West and the Russian Federation against the background of the Ukraine crisis certainly has a negative impact on the process of resolving the frozen conflicts in the region, Transnistria included. Therefore, the cut-off of the dialogue in this respect and the heightening of separatist tensions in Transnistria add to the challenges Romania has to cope with. Transnistria represents one of the strongest levers the Kremlin could use to destabilise the Republic of Moldova, with grave repercussions on Romania's security.

Even more, the increasingly solid Russian-Serbian relations, the increasingly clear Belgrade's tendency to enhance its partnership with Moscow, often in the detriment of the EU (for instance, its involvement in *South Stream* project or the attitude in the Ukrainian crisis context) amplify the complexity of security challenges in Romania's vicinity, being clear examples regarding their cross-cutting nature. Geo-economic evolutions are some of the Ukraine crisis' key-points, with considerable relevance for the Western Balkans, as well as for Romania, especially if we have in view that the Black Sea area has had, even before the Ukrainian crisis, a great geo-economic value.

Also, a recent *Economist Intelligence Unit* report clearly refers to Romania's vulnerability from the perspective of its relations with Russia, in conjunction with the geographical location of our state. Thus, the document emphasises that Russian-Romanian relations, uneasy anyway, have become tenser under the conditions in which Bucureşti has been one of the most vehement voices requiring the toughening of sanctions for Russian actions in Crimea. However, despite the reduced energy and trade dependency on Moscow, due to its geographical location and its relations with the Republic of Moldova and Ukraine, as well as Romania's foreign policy interests regarding the Republic of Moldova, our country *"has the highest level of vulnerability regarding the possibility of the emergence of a conflict of foreign policy interests with the Russian Federation"*[30].

[30] ***, *Country Report. Romania, Economist Intelligence Unit*, UK, November 2014, p. 4.

The energy area is one of those in which the Ukrainian crisis repercussions are reflected in a clear manner. Although, by comparison with most European states, Romania has a low level of dependency on imports from Russia (for instance, in 2010, Romania imported 22% of its necessary of energy, most of it from Russia)[31], the dependency on Moscow, even though low, represents one of the major economic vulnerabilities, under the conditions in which the Kremlin used in the past the disruption of natural gas delivery as a means of achieving political interests. This makes it necessary to hasten the efforts for identifying alternative sources of import and to support the European initiatives in this respect.

Moreover, Russian annexation of Crimea determines a change in the strategic balance within the Black Sea basin. If, before 18 March 2014, Moscow controlled only Sevastopol, the main base of the Russian fleet in the Black Sea, and two additional naval bases, presently, Moscow controls hundreds of kilometres of coast in Crimea and in the adjacent waters, at the border of Romania, NATO, and the EU.

In this respect, at the Wales Summit (2014), it was decided the approval of *NATO Readiness Action Plan (RAP)*, a plan meant to increase the Alliance's operational capacity, which also includes measures for the Allies strategic reassurance[32], especially those on its Eastern flank – the Baltics, Poland, and Romania. Besides these measures, it is also noteworthy the increase in Romania's defence budget, which is planned to reach the threshold of 2% until 2017.

The importance of reassurance measures is even higher in the context in which the regional political-military cooperation formats, *BlackSeaFor* and *Black Sea Harmony*, proved, in the context of the Ukraine crisis, their limits, being currently paralysed.

The analysis carried out within the present article reveals the need for changing the manner in which we relate to national security, within the region Romania is placed. This time, the emphasis is not placed on the security guarantees as a result of its belonging to the Euro-Atlantic security community, but on Romania's responsibilities as a result of the same quality. In our opinion, it means that international

[31] ***, *European Economy. Member States' Energy Dependence: An Indicator-Based Assessment*, Occasional Papers 145, Directorate-General for Economic and Financial Affairs, April 2013, pp. 225-226, see http://ec.europa.eu/economy_finance/publications/occasional_paper/2013/pdf/ocp145_en.pdf, retrieved on 3 June 2015.

[32] According to the *Wales Summit Declaration*, these measures include the continuous air, land, and maritime presence and meaningful military activity in the Eastern part of the Alliance, both on a rotational basis. These will provide the fundamental baseline requirement for assurance and deterrence, and are flexible and scalable in response to the evolving security situation. For details, see: *Wales Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales*, 24 September 2014, http://www.nato.int/cps/en/natohq/official_texts_112964.htm, retrieved on 8 June 2015.

relations have got to the stage of typical realist thinking, replacing more and more obviously the idealist vision having marked international affairs during unipolarity, until the emergence of the world economic and financial crisis.

The Western Balkans and the Black Sea area, although different from the perspective of the relations with great powers, of their historical and cultural backgrounds, delineate to be, within the present study, a space crossed by numerous connections, functioning as drivers of instability, subjected to contrary forces, generating tensions which can result, as the recent events attest, in regional crises with a high potential to get a trans-regional character.

The Ukraine crisis asserts, beyond question, the major strategic importance of the Black Sea from political, military and economic points of view, revealing the limits of the cooperation initiatives carried out until now, the contagion potential of instability at trans-regional level, as well as the clear need for the development of new strategic visions not only at NATO and EU levels, but also at Romania's level, adapted to the new regional context. Under these circumstances, Romania plays or should play a fundamental role, being the outpost, the spearhead of promoting stability in the region.

References

1. ***, *The Military Balance 2014*, Chapter Five: Russia and Eurasia, Routledge Publishing House, London, 2014, pp. 161-200.

2. Vladimir Pasti, *Să recunoaştem statul Kosovo? Nu. De ce?,* in *Foreign Policy Romania*, no. 14, January/February 2010.

THE STRATEGIC PARTNERSHIP BETWEEN ROMANIA AND THE USA

– A Cornerstone in the Current Security Context –

Daniela RĂPAN

Given the worldwide importance of the United States of America and, consequently, the significance of the cooperation relations that a country can enjoy with such a major partner, the author considers that it is particularly relevant to carry out a case study of the diplomatic relations between Romania and the USA in the field of defence. The article includes a short history of bilateral cooperation and emphasises the strands of cooperation, with a special focus on the defence component. The author concludes that the Strategic Partnership between Romania and the USA is a solid proof of the enhanced bilateral cooperation in fields of strategic interests, conveying a unique status to our country in the regional context.

***Keywords**: Romania; the USA; foreign policy; strategic partnership; bilateral relation; security challenges*

Introduction

In Romania's foreign policy, particular attention is attached to bilateral strategic partnership with twelve countries[1], namely Azerbaijan (since 2009), China and South Korea (since 2008), France (also since 2008), Italy (since 1997), Japan (since 2002), Poland (2009), the United Kingdom of Great Britain and Northern Ireland, Spain (2013), the USA and Turkey (since 2011) and, last but not least, Hungary (2002). After studying official documents, I find that most of these partnerships also include the aspect of security and defence.

Given the worldwide importance of the United States of America and, consequently, the significance of the cooperation relations that a country can enjoy with such a major partner, I believe it is particularly relevant to carry out a case study of the diplomatic relations between Romania and the USA in the field

Daniela Răpan – expert, Centre for Defence and Security Strategic Studies, *"Carol I"* National Defence University, București.

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

[1] A.N.: these countries are listed alphabetically.

of defence. As announced in the abstract, the case study includes a short history of bilateral relations and reviews the strands of cooperation, with special emphasis on the defence component.

Evolution of Bilateral Relations

I appreciate that a brief historical insight into the evolution of bilateral relations along the 135 years of diplomatic cooperation is useful to my endeavour.

Regarding the beginning of bilateral relations, Romania established diplomatic relations with the United States of America in 1880. They were interrupted in 1941, during the Second World War, but they were subsequently resumed in 1946 and upgraded to Embassy level in 1964.

Initially, the US representation in Romania was established at the level of diplomatic agency, created on 14 June 1880, but after only two months, Secretary of State W. M. Evarts decided to upgrade the US level of representation in Bucureşti to legation level. Thus, Eugene Schuyler, a leading figure of that time, was appointed diplomatic agent and Consul General for a four-year term in Romania (also being accredited in Serbia and Greece, where he had the residence). Schuyler was one of the first American citizens who became a Doctor of Philosophy. He could speak both Romanian and Russian. Moreover, he published a series of articles about the Romanian literature in the renowned American magazine *"The Nation"*; he was also appointed member of the prestigious Romanian Academy of Sciences. In my opinion, the appointment of such a representative can be an indication of the importance attached by the USA to the countries in this region and, particularly, to Romania.

The first diplomatic mission of a Romanian representative in the USA and, at the same time, the first Romanian diplomat officially received at the White House was Colonel Sergiu Voinescu, as Special Envoy of Prince Carol, on 18 November 1880. The diplomat announced publicly, in front of the US President at the time, Rutherford B. Hayes, Romania's independence and its international recognition.

Starting in 1905, the residence of the American diplomatic representative was established in Bucureşti, being also accredited for Serbia and Bulgaria.

As regards Romania's participation in the First World War, Woodrow Wilson, the US President at the time, sent King Ferdinand (as Romania was a US ally country) a message in which he made the following statement: *"US citizens have watched, with their warmest sympathy and admiration, the brave fight that Your Majesty and the Romanian people have put up to protect your country's integrity and national freedom from the domination of German militarism"*.

In the interwar period, the US diplomatic representation had exclusive accreditation in our country.

As, later on, during the Second World War, Romania joined the Axis Powers (Italy, Germany, Japan), its diplomatic relations with the USA were interrupted and subsequently resumed in 1946, at the level of Legation.

Almost two decades later, in 1964, the diplomatic relations were upgraded to embassy level and then a period of cordial relations followed, with exchanges of formal visits at presidential level.

In 1975, a Trade Agreement was concluded, by which our country benefited from the most-favoured-nation clause[2]. This was largely owed to our country's option not to join the Warsaw Treaty countries in invading Czechoslovakia in 1968, Romania having an individual position within the Soviet bloc.

During the second half of the 1980s, bilateral relations became more distant (Romania lost the status granted by the most-favoured-nation clause), against the background of the reluctance of the Romanian communist regime to grant fundamental rights to its citizens.

But after the 1990s, when the political regime changed, relations between Bucureşti and Washington became good once again, being developed at a slow pace, the USA manifesting an *"attitude of expectation, observation and understanding"*[3].

It can be said that the bilateral relations in the field of defence have also been constantly developed.

Thus, on 1 April 1993, Mil-to-Mil Program was initiated, aiming to get Romanian military familiarised with the US military structures, personnel, top management, training and equipment[4].

To be noted that ever since NATO launched the Partnership for Peace (PfP) programme, in 1994, Romania expressed its interest to become a member, with a view to subsequently joining the North Atlantic Alliance, which had a great significance for the reassessment of the American perception. Romania was the first country in the former Communist bloc[5] to become a member of this structure.

[2] Alex Ciungu, *Relaţia România-SUA – realităţi şi perspective geopolitice*, p. 4, see http://alexciungu.wordpress.com/, retrieved on 3.04.2015.

[3] Alexandru Grumaz, *România-SUA. 130 de ani de relaţii diplomatice*, 29 June 2010, see http://www.alexandru-grumaz.ro/, retrieved on 3.04.2015.

[4] According to *Carta Albă a Apărării*, Chapter II, see http://www.mapn.ro/diepa/text/cartaalba/capitolul2.pdf .

[5] For details, see the table with the dates of signature to the documents for accession to the Partnership for Peace, available at http://www.nato.int/cps/en/natolive/topics_82584.htm, retrieved on 3.04.2015.

Moreover, the efforts made by our country to strengthen democracy and reform economy, as well as the assertion of fundamental human rights led the American authorities to grant Romania back the most-favoured-nation clause in 1996.

On 11 July 1997, during the official visit of the US President, Bill Clinton, to Bucureşti, the *Strategic Partnership* between the two states was launched. Since then, it has been a cornerstone of the foreign policy for the Romanian authorities and, at the same time, an efficient instrument supporting domestic efforts to reform the political, economic, military and administrative fields, with a view to joining the Euro-Atlantic organisation, as well as to promote our country as a stability and security factor in South-Eastern Europe.

Due to the close bilateral cooperation to fight non-conventional threats (such as trafficking in drugs or human beings, financial crime and other types of crimes), but also to the importance attached to this cooperation by both parties, on 20 May 2001, an agency of the Federal Bureau of Investigation (FBI) was set up in Bucureşti.

After the attacks of 11 September, our country showed a quick and firm reaction, expressing its entire availability to join the USA in the fight against terrorism. Thus, Romania became a staunch ally of the *primus inter pares* country in NATO. Its support was reflected in its participation in the military operations in Afghanistan and Iraq. Moreover, the two countries cooperated more closely in taking specific actions in order to combat terrorism.

Thus, on the one hand, the positive results achieved by Romania concerning the economic reform[6] and, on the other hand, the concrete contribution of our country to the fight against terrorism were the main elements that led to the US support for Romania's accession to NATO. As it is well known, Romania joined NATO eleven years ago, on 29 March 2004.

Another benchmark of the evolution of bilateral relations, which I believe it is worth mentioning, is the signing, on 6 December 2005, of the Agreement between the United States of America and Romania regarding the activities of the United States Forces located on the territory of Romania, also called the *"Access Agreement"*[7] (the act came into force on 21 July, the following year).

[6] To be also noted that, in 2003, Romania was granted the status of *"market economy"* by the US authorities.

[7] This Agreement functions on the basis of a complex legal framework and specialised structures established within the Romanian central administration.

The permanent military presence on Romania's territory, near the Black Sea, is a concrete result of this Agreement. In this respect, I would note the *Black Sea Rotational Force* initiative, dating back in 2010, the military base located in Mihail Kogălniceanu hosting troops rotating every six months, which develop multinational military exercises and common training activities.

In 2010, when 130 years of diplomatic bilateral relations were celebrated, the Romanian Parliament and the US Congress adopted resolutions reaffirming the preservation of the commitment made by both parties to constantly contribute to strengthening the relation of strategic partnership.

In the same year, on 17 June, during the visit to Bucureşti by Ellen Tauscher, Undersecretary of State for Arms Control and International Security Affairs, negotiations were initiated concerning the legal framework regulating the deployment on the Romanian territory of the US missile defence system elements (*Ballistic Missile Defence System – BMD*) in Europe.

The *BMD* bilateral agreement[8] was signed on 13 September 2011, by the Romanian Minister of Foreign Affairs and the American Secretary of State, in the context of the visit of the Romanian President to Washington, and entered into force on 23 December, the same year.

At the same time, on the very day of signature of the *BMD* Agreement, the *Joint Declaration on Strategic Partnership for the 21st Century* between Romania and the United States of America was also adopted, confirming the excellent long-term, continuously developing Partnership between the two states, establishing at the same time the pillars of the bilateral relation: *"political dialogue, security, economy, people-to-people contacts, science and technology, research, education, culture"*[9].

Against the background of the *Joint Declaration* adoption, it was decided to set up working groups (WG, or the so-called *task forces*), among which I mention the WG dedicated to consular aspects, including visas, the WG dedicated to economic and commercial areas, and the WG dedicated to energy security.

Considerations on the Missile Defence System

Referring to the Missile Defence System in Deveselu, achieved by means of the US programme entitled *European Phased Adaptive Approach – EPAA*, it is meant to ensure a better protection of the forces deployed in Europe

[8] For details and clarifying notes, see Bogdan Aurescu, *Article by Article Commentary of the Text of the Agreement between Romania and the United States of America on the Deployment of the US Ballistic Missile Defence System in Romania*, in *Strategic Impact* no. 3 [44]/2012.

[9] According to the data provided by the Ministry of Foreign Affairs, see http://www.mae.ro/print/4944, retrieved on 4.04.2015.

and in the theatres of operations where the US and allied troops are employed, on the one hand, and of the populations and territories of the USA and its allies. The agreement provides that, once the system becomes operational, it shall be controlled by NATO and the Base in Deveselu shall become a base of the Alliance.

This aspect is justified and supported by the idea taken from the *Strategic Concept* of the Alliance currently in force[10], according to which NATO shall develop the capability to defend populations and territories against ballistic missile attacks, as a core element of collective defence, which contributes to the indivisible security of the Alliance[11].

Although the project has caused considerable adverse reactions from the Russian Federation – which, perceiving it as a threat to its national security, has requested legal guarantees that the goal of the missile defence system is not the annihilation of its nuclear strategic potential – it continues to be put into practice, being intended to be completed during this year.

The need for this project, which I share, is motivated by the fact that, *"at the level of the European continent, there is no coherent, well-rounded system of defence against possible ballistic missile attacks"*[12] and that, taking into account the high degree of development of state-of-the-art technologies used in the military field, several state actors have created a system of medium-range and long-range ballistic missiles.

According to the declarations made by US officials, the defence system is meant to ensure protection from threats from Iran. Of course, the two states cannot be compared in terms of power, but it should be mentioned that Iran enjoys support from other states in the region that possess nuclear weapons (Russia, China and North Korea).

This way, the missile defence system can be interpreted as the expression of a policy of intimidation, deterring possible threats from Iran to US allies (for instance, Israel) and to NATO forces acting in the region[13].

[10] The official text of the *Strategic Concept* adopted in Lisbon in November 2010 is available at http://www.nato.int/cps/en/natolive/official_texts_68580.htm.

[11] *Strategic Concept*, Title *"Defence and Deterrence"*, paragraph 19.

[12] Petre Duţu, Daniela Răpan, *Implications of the Anti-ballistic Missile Defence System in Europe on Russia-USA Relations*, in *Strategic Impact*, no. 3/2011, p. 33.

[13] Teodor Frunzeti, *Echilibrul ameninţării şi echilibrul de putere*, in Petre Duţu (coordinator) *International Scientific Paper Session* organised by the Centre for Defence and Security Strategic Studies, Editura U.N.Ap, Bucureşti, 2011, p. 22.

Considerations concerning the Strategic Partnership

A strategic partnership between two states relies on diplomatic relations based on trust, reciprocity and enhanced cooperation, especially in those fields viewed as being of strategic interest.

Bearing in mind the aspects mentioned throughout the paper, it can be concluded that the partnership between Romania and the USA is a viable strategic one, for several reasons.

The first aspect is the temporal one – it has been a 135-year history of diplomatic relations between the two countries, a period during which they have developed and strengthened. A second aspect is represented by the complexity of the fields of cooperation: political, economic, military and security, people-to-people relations, science and technology, research, education and culture. The third and the most powerful argument in this respect is the consistency of the security and defence component (military field).

I also note that a complex legal framework has been developed between Romania and the USA, which regulates various fields of activity, being constantly updated depending on the developments in the area of bilateral relations or at global level. This legal framework is made up of treaties, agreements and a series of technical arrangements[14] concluded both at government level and at the level of agencies.

Conclusions

After analysing the diplomatic relations between Romania and the USA in the field of defence, it can be noted that Romania and the USA enjoy *"exceptionally strong military relations"*, a fact which is also emphasised by the American diplomatic representative[15]. A relevant argument is the fact that the armed forces of the two countries participate together in numerous military exercises, many of which in Romania [16], in coalition military operations such as the ones in Iraq and Afghanistan and, last but not least, in expeditionary missions throughout the world, within NATO framework.

[14] A list of these arrangements is available at http://www.mapn.ro/diepa/, retrieved on 3.04.2015.

[15] The declaration of the US Embassy on military relations with Romania, 16 September 2013, Deveselu (Lucian Crusoveanu/Public Diplomacy Office), see http://romania.usembassy.gov/media/pr-09162013.html, retrieved on 03.04.2015.

[16] Every year, Romanian soldiers undertake exercises jointly with American soldiers; within the years 2014-2015, a series of such exercises have been carried out at the level of all three armed forces services. For details, see articles in the media, http://www.ziare.com/articole/exercitii+militari+romani+americani, retrieved on 3.04.2015.

At the most recent Annual Meeting of the Romanian Diplomacy, the Minister of Foreign Affairs has stated that the bilateral relation with the United States of America is and will remain the keystone of our foreign policy, while the political-military dimension remains a priority within the bilateral relation, in the light of the enhanced presence of the United States in Romania and the Black Sea[17].

To conclude, I consider that the Strategic Partnership between Romania and the USA is a solid proof of the enhanced bilateral cooperation in fields of strategic interests, conveying a unique status to our country in the regional context.

Selective Bibliography

1. Radu Dan Septimiu Popa, *Partneriatul strategic cu SUA. Fundamente pragmatice pentru securitatea naţională a României*, in *Securitatea şi apărarea spaţiului sud-est european, în contextul transformărilor de la începutul mileniului III* – Volume of the International Scientific Paper Session *Strategii XXI*, Section 3 – National Defence and Security, 13-14 April 2006, Editura Universităţii Naţionale de Apărare *"Carol I"*, Bucureşti, pp. 406-423.

2. Valentin Simion, Doctoral Thesis, *Evoluţii privind securitatea europeană. Prezenţa militară americană în România, implicaţii la nivel naţional şi zonal*, *"Carol I"* National Defence University, Bucureşti, 2012, pp. 117-128.

3. NATO Official website, http://www.nato.int.

4. Official website of the Romanian Ministry of Foreign Affairs, http://www.mae.ro

5. ***, press articles, http://www.ziare.com/articole/exercitii+militari +romani+americani

[17] Minister (at the time) of Foreign Affairs, Titus Corlăţean declaration in the official opening of the Annual Meeting of the Romanian Diplomacy on 27.08.2014, see http://www.mae.ro/node/28262, retrieved on 4.04.2015.

RUSSIA AND THE PIVOT TO ASIA (II)

Silviu PETRE

During the Cold War, the Soviet Union's involvement in the Vietnam War was justified in the name of countering the US intervention and materialised in the form of supplying weapons or sending military advisers. In turn, the Viet Cong capitalised on the involvement of Moscow to counter China's regional claims. The author opines that, after 1991, the Russian Federation interest in the coastal nation has greatly diminished but it has never totally disappeared, especially as Russia had a military base at Cam Ranh Bay. Although Russia waived the right to use the base, it has not completely lost the interest in the region. A piece of evidence in this regard is the strategic partnership signed with Hanoi in 2001.

***Keywords**: regional power; terrorism; national reconstruction; Myanmar*

Russia in Bangladesh

The relations between the Soviet Union and Bangladesh got consolidated during the *Cold War* as the red superpower supported the birth of a new state that, by its existence, weakened the power of Pakistan, the US ally. Besides quickly recognising it, Soviet engineers got involved in the country post-conflict reconstruction, especially in the energy sector. We mainly refer here to the thermal power plants in Siddhirganj and Ghorasal, dating from the mid-'70s, the latter being currently modernised[26]. Moreover, the asset that should place Bangladesh among the emergent powers in the 21st century is represented by civil nuclear energy. There have been plans to build a nuclear power plant since 1961. In 1963, following several feasibility studies, the place chosen to build it was Rooppur, in Pabna district, 200 km north of Dhaka. In 1980, the government approved the plan for the future plant having an estimated capacity of 125 MW. The plans remained on paper for decades, proving the nation structural weaknesses. They were close to being implemented after 2000, when the elites in Dhaka considered the offers made by different actors: China, Russia, South Korea. Moscow won the lottery ticket in May 2009, the governments of the two states signing a memorandum of understanding to regulate the future collaboration.

Silviu Petre – researcher, Centre for East European and Asian Studies, National School for Political Studies and Public Administration, Bucureşti.

[26] Nurul Islam Hasib, *Russia Coming Back to Bangladesh*, BdNews24, 8 March 2014.

The document was strengthened by another intergovernmental agreement signed in May 2010 by Sergei Kiriyenko, Director of the state-owned company *Rosatom*, and Yafesh Osman, Minister of Energy in the host country[27]. The Russian proposal was to build two 1000 MW AES-92 nuclear plants in Rooppur up to 2017. The initial company that was to bear the burden of building the plant was *AtomStroyExport*, which was then absorbed by *Nijny Novgorod Atomenergoproekt (NIAEP)*. The technical characteristics of the plants that would supplement Bangladesh energy needs are listed in *table 1*[28].

Table 1

Name	Type	Capacity	Beginning of construction	Beginning of exploitation
Rooppur 1	AES-92	1000 MWe	2015	2020
Rooppur 2	AES-92	1000 MWe	2020	2025

As any emerging power should consider all the dimensions of its assertion to be a factor that is taken into account, the military element has not been neglected. Dhaka-Moscow *rapprochement* has been grafted onto the already existing friendship between Russia and India. Sheikh Hasina Government, pro-secular and pro Indian, which took office in 2009, responded to Putin regime courtesy. The visit at the Kremlin in January 2013 resulted in the greatest military contract in the history of the South-Asian nation. Bangladesh received a $ 1 billion loan to purchase a wide range of post-Soviet technology: from armoured vehicles to anti-aircraft systems and M-17 helicopters. Intimacy seems to have grown so much that some Indian analysts wonder whether Dhaka foreign policy has become Russo-centric, as noticed by Harun ur Rashid, former Ambassador of Bangladesh to Geneva[29].

On the other hand, the Russian Ambassador accredited to Dhaka, Alexander Nikolaev, talked about the revival of the relationship between the two countries, while ensuring that his country came in Southeast Asia to remain for a long period of time, profession of faith that epitomises Russia's pivot to Asia[30].

Russia in Myanmar

A state on the border between South Asia and Southeast Asia, Myanmar seems small compared to the surrounding giants but, actually, it is larger and more populous than many European states. Its territory of over 670,000 square km is the home

[27] *Russia and Bangladesh Agree to Cooperate*, World Nuclear News, 21 May 2010.

[28] *Nuclear Power in Bangladesh, World Nuclear Association*, June 2014, see http://world-nuclear.org/info/Country-Profiles/Countries-A-F/Bangladesh/

[29] Arafat Kabir, *Crimea and Bangladesh: Behind the Controversy*, *The Diplomat*, 10 April 2014. Harun ur Rashid, Is Bangladesh's Foreign Policy Becoming India and Russia-centric?, IPCS, 15 April 2014.

[30] Nurul Islam Hasib, *ibidem*.

of over 60 million inhabitants who can hardly be said to form a nation. The intolerance resulted from diversity has hindered the state-building project. Under the iron fist of the former military junta in Rangoon (since 2011, the capital is Naypyidaw) numerous points of rebellion have occurred, claiming more autonomy or even total separatism. The problem of Rohingya Muslim ethnic minority who flee to India has been internationalised, placing Myanmar under the international community scrutiny.

Here Russia intervenes. The former Soviet Union provided the military command with three helicopters in 1963. In 2009, as a sign of resuming relations, Moscow sold Myanmar a $ 570 million contract in the form of 20 MiG-29 aircraft, together with their piloting expertise. To them were added Mi-35 attack helicopters, training aircraft and artillery assets. Additionally, the aviation in Myanmar received flight lessons from the one in India, its neighbour, not to be outdone by the great ally in the north, not to mention that the Indian military personnel used to be more familiar with Russian technology[31].

Three years later, in 2012, news agencies demonstrated that the Russian military diplomacy was only the spearhead of other economic long-term interests. *OAO Gazprom (OGZD)*, a company controlled by the state, took advantage of the cancellation of the sanctions imposed by the United States to exploit the mineral resources of Myanmar[32].

Russia and Sri Lanka

At a first glance, the small Lankan Island (*Sri* being a title of courtesy) should be a tourist paradise and nothing more. Unfortunately, the ethnic-economic problems between the Sinhalese majority and the Tamil minority as well as the maritime position in the Indian Ocean have contributed to its tumultuous destiny in the past thirty years. The important role it plays for India, the United States and, more recently, China not only provides it with important investments but also consolidates the peace brought by the Mahinda Rajapaksa regime using the sword. This is because, despite the interests in human rights, many investors, together with the governments behind them, are ready to close their eyes to the authoritarianism in Colombo as long as there are business opportunities. Russia is not an exception, following the same logic. In mid-June, Russian Ambassador to Sri Lanka, Alexander Karchava, praised the efforts made by Rajapaska Government to counter terrorism

[31] Rakesh Krishnan Simha, *Rangoon Realpolitik: Russia, India Courting Myanmar*, *Russia&India Report*, 31 January 2014, see http://in.rbth.com/blogs/2014/01/31/rangoon_realpolitik_ russia_india_courting_myanmar_32723.html

[32] Stephen Bierman, *Russian Companies Hold Talks with Myanmar Developing Oil Ties*, Bloomberg, 28 September 2012.

and to get involved in national reconstruction. The Russian official spoke about his country's willingness to expand cooperation beyond the bilateral traditional domains of technology, construction, and trade[33]. The gesture should not be interpreted only in the context of usual protocol, as Karchava's speech was preceded by the visit of other Russian officials, including the Head of Gazprom, Gulev Valeriy, who, in August 2011, met the President's brother and Minister of Development, Basil Rajapaksa, to point the routes of extraction of the oil resources in Mannar and Cauvery Basin[34].

In mid-March 2014, the Lankan press discussed the visit of Felix Komarov, a businessman who wanted to break the ground for new investments. Subsequently, Komarov became the owner of *Ceylon Tea*, wanting to change its logo[35].

Russia and Vietnam

American films about Southeast Asia present the past and not the present. Having a population of about 100 million inhabitants and an economic growth rate of 6% per year before the crisis, Vietnam should be considered as far as the dynamics of the region is concerned. Situated in the vicinity of the disputes in the South China Sea, it is actually part of, the state having the capital in Hanoi is in the ring of fire of the geopolitics in the Pacific. America, India and China include it in their regional power equations.

Recently-discovered oil reserves are estimated at 4.4 billion barrels (January 2013). By comparison, Vietnam is ranked third among oil producers in Asia, after China and India. However, oil industry is working below potential, as suggested by the figures provided by the US Energy Administration: therefore, in 2012, production was 364,000 barrels per day, down from 404,000 barrels per day, as it was in 2004[36].

Map of Oil Exploitation in Vietnam

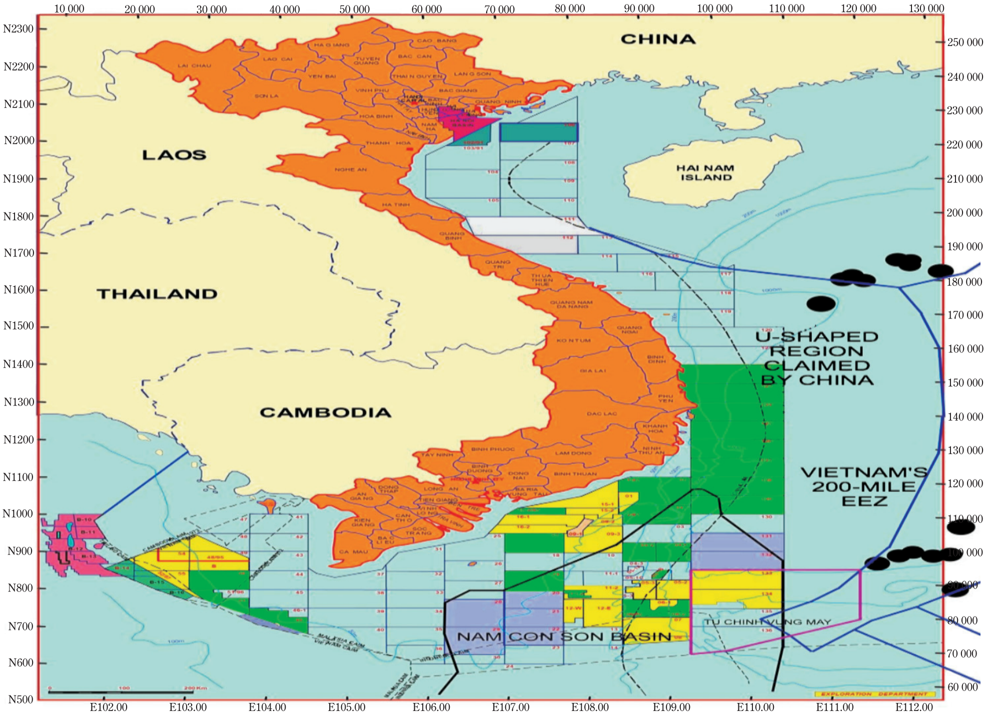
It goes without saying that Hanoi is ready to enter into contracts with the foreign companies willing to develop the already existing infrastructure. The website of the state company *PetroVietnam* denotes a global presence, a sign of the emerging power that is Hanoi.

[33] *Russia Lauds Sri Lanka's Handling of Post Conflict Issues*, Ministry of Defence and Urban Development, 6/12/2014, http://www.defence.lk/new.asp?fname=Russia_lauds_Sri_Lanka_handling_of_post_conflict_issues_20140612_01

[34] A.A.M. Nizam, *Russian Business Giant "GazProm" is to Open its Office in Sri Lanka Next Month*, *Asia Tribune*, 17 August 2011.

[35] *Russian Investor Felix Komarov Visits Sri Lanka*, FT Lanka, 14 March 2014.

[36] US Energy Information Administration, Vietnam, data last updated: 30 May 2013, see http://www.eia.gov/countries/country-data.cfm?fips=vm



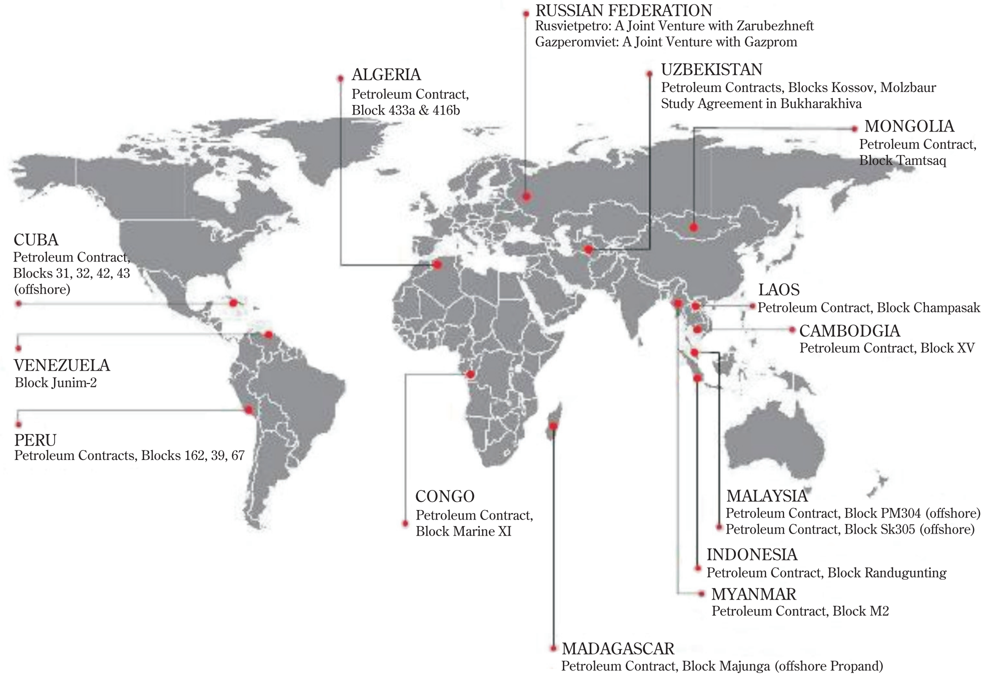
Source: *Great Game in the South China Sea*, in *The Hanoist*, 16 April 2012, see http://thehanoist.wordpress.com/2012/04/16/great-game-in-the-south-china-sea/

During the *Cold War*, the Soviet Union's involvement in the Vietnam War was justified in the name of countering the US intervention and it got materialised in the form of supplying arms or providing military advisers. In turn, Viet Cong took advantage of Moscow's presence to counter Mao's China regional claims. After 1991, the Russian Federation interest in the coastal country has significantly diminished, but it has not totally disappeared, especially as Russia had a military base in Cam Ranh Bay. Its fate was discussed following a bilateral meeting in 1998[37]. Russia waived its right to use the base without leaving the region completely. The evidence was the strategic partnership signed with Hanoi in 2001. In 2012, its level was raised from *standard* to *comprehensive*. In the spring of this year, Russia promised to deliver Vietnam twelve *Suhoi SU-30MK2* aircraft that can hit ground and naval targets; they were added to another contract related to six *Varshavyanka* submarines, *Kilo* class improved ones.

On the civil side, *Gazprom* has been leased 49% of two blocks in the South China Sea, which are believed to shelter 1.9 trillion cubic feet of oil (US measurement)

[37] Greg Austin, Alexey D. Muraviev, *The Armed Forces of Russia in Asia*, I.B.Tauris, New York, 2000, p. 119.

Oil and Gas Exploration and Production Projects Worldwide


RUSSIAN FEDERATION
Rusvietpetro: A Joint Venture with Zarubezhneft
Gazperomviet: A Joint Venture with Gazprom
ALGERIA
Petroleum Contract,
Block 433a & 416b
UZBEKISTAN
Petroleum Contracts, Blocks Kossov, Molzbaur
Study Agreement in Bukharakhiva
MONGOLIA
Petroleum Contract,
Block Tamtsaq
CUBA
Petroleum Contract,
Blocks 31, 32, 42, 43
(offshore)
LAOS
Petroleum Contract, Block Champasak
CAMBODGIA
Petroleum Contract, Block XV
VENEZUELA
Block Junim-2
PERU
Petroleum Contracts, Blocks 162, 39, 67
CONGO
Petroleum Contract,
Block Marine XI
MALAYSIA
Petroleum Contract, Block PM304 (offshore)
Petroleum Contract, Block Sk305 (offshore)
INDONESIA
Petroleum Contract, Block Randugunting
MYANMAR
Petroleum Contract, Block M2
MADAGASCAR
Petroleum Contract, Block Majunga (offshore Propand)

Source: *Petrovietnam*, official data, http://english.pvn.vn/?portal=news&page=detail&category_id =38&id=3676

and 25 million tons of gas in solid state[38]. Moreover, it is estimated that, in Vietnam, the first civil nuclear plant will be built using Russian technology by 2024. Prime Minister Medvedev, who visited Vietnam in early November 2012, announced that his country would pump 10 billion in the project. During the same meeting, the Vietnamese counterpart, Nguyen Tan Dung, expressed the hope that Hanoi would sign a free trade agreement with the customs union formed by Russia-Belarus-Kazakhstan[39].

Instead of a Conclusion

To use a metaphor, the sun rises in the East, but it is not always sunny.

Russia's pivot to Asia has much to reveal, even beyond the intentions of its initiators in the Kremlin. President Putin's *Oostpolitik* should not be regarded too optimistically, as there may be a lot of surprises. Even if the energy contract with China and the diplomatic pirouettes to the warm waters of the South provide a respite

[38] Stephen Blank, *Russia and Vietnam Team up to Balance China*, in *The National Interest*, 7 April 2014.

[39] Stephen Blank, *Russia's Ever Friendlier Ties to Vietnam – Are They a Signal to China?*, in *Eurasia Daily Monitor*, Volume: 9 Issue: 219, 30 November 2012.

from the crisis in Ukraine and the Western pressure, Asia brings not only privileges but also obligations.

❖ Firstly, signing cooperation with China will not be comfortable at all, and the economic and financial benefits obtained in the short term will count in changing the balance of power in the long term. In this context, mention should be made that Beijing has already had a potential well above that of Russia. Except nuclear arsenal, the Middle Kingdom dominates in all areas, and it hurries to bridge the gap for the chapters it lags behind. Boycotting European products, Moscow only replaces an inter-dependence with another and nothing more![40].

❖ Secondly, Central Asian nations might not be very keen on the scrutinising eye of their great neighbour in the North. As shown in an article written for the Indian think-thank, *IDSA*, Kazakhstan and Kyrgyzstan have serious concerns about the possibility to experience, in time, the same scenario as Ukraine, especially as there are ethnic Russians on their territory[41].

❖ Thirdly, the contract with Pakistan, Sri Lanka or Vietnam could bring Russia in a state of friction with China and India, allies (especially the latter) Russia needs to justify the ideology of multipolarism. Moreover, if Putin Administration and its successors want to have a word that carries weight in the region, they will have to provide public benefits or to involve in managing latent or manifest tensions, which is to complicate their lives! The Americans have learned the hard way how complicated Asian files can be...

❖ Fourthly and for the moment the last: we usually talk about states and inter-state relationships, forgetting that there are also other actors in the world, often more important. As we have mentioned above, the flags of Russian oil companies have been flying in different points such as the South China Sea rim. It is known that one of the problems of the Russian economy as well as of other oil- authoritarianisms refers to the excessive reliance on raw mineral resources. The new South-Southeast Asian investment opportunities could maintain this state of affairs and benefit only some state-owned companies and the few people involved in extractive industry, and not the population as a whole.

Selective Bibliography

1. Stephen Bierman, *Russian Companies Hold Talks with Myanmar Developing Oil Ties*, Bloomberg, 28 September 2012.
2. Baqir Sajjad Syed, *Kayani to Visit Russia from 3 Oct*, *Dawn*, 29 September 2012.
3. Ekaterina Stepanova, *Afghanistan after 2014: The Way Forward for Russia*, *IFRI*, May 2013.
4. P. Stobdan, *Post-Crimea: Central Asian Fear Putin's Stick*, *IDSA*, 4 August 2014.

English version by
Diana Cristiana LUPU

[40] Elena Dumitru, *Analiză. Putin distruge economia rusă doar pentru a sfida Vestul. Rusia nu poate supravieţui fără importurile din UE şi SUA*, in *Adevărul*, 7 August 2014.

[41] P. Stobdan, *Post-Crimea: Central Asian Fear Putin's Stick*, *IDSA*, 4 August 2014.

CYBERSPACE SEMANTICS AT NATO LEVEL

Colonel Dr BEng Dan COLESNIUC
Major Marian TURLEI

One of NATO responsibilities is represented by the analysis of the current or ongoing threats to member countries. A series of events have revealed that cyber activities can affect both national and transatlantic prosperity, security and stability. In this context, the authors consider that terminology should be defined for unitary semantics within the Alliance. Moreover, a pattern connected to the level of cyber threats should be introduced. This approach will determine an objective assessment of threats and will enable issuing correct political-military decisions. The authors conclude that, given the challenges created by the virtual space, NATO must play a significant role. Therefore, cyber semantics is essential in the light of the initiatives related to diminishing the development of prospective conflicts launched from the cyberspace.

***Keywords**: NATO; cyberspace; cyber semantics; cyber conflict; cyber defence*

NATO and the Cyberspace

In the media reports regarding the worst scenarios connected to the virtual space a series of concepts are always encountered, such as: *"Cyber-warfare: Hype and fear"*, *"Cyber-security: War on terabytes"* or *"Escalating cyber-attacks – It's about time"*.

From the military perspective, the choice of previous definitions is somehow justifiable, suggesting that there are in fact major security challenges that NATO has to deal with.

Cyberspace is not a physical environment, but a virtual one, being more than what the Internet can represent. Moreover, it comprises computer networks and everything that contributes to connecting and controlling them. The environment is characterised by the use of electronic devices, such as computers needed for storing, processing and exchanging data, both on the Internet and within the restrictive networks. Thus, the prefix "*cyber*" defines everything connected to the *cyberspace*.

NATO attaches great importance to the security in the cyberspace, as compared to other authorities and companies, whose work is focused on finding an IT infrastructure. NATO comprises 30 significant communication networks and over 100,000 computers. A secure cyberspace is essential not only for immediate

Colonel Dr BEng Dan Colesniuc, Major Marian Turlei – the Ministry of National Defence.

objectives, determined by the need for communication, but also for the systems and equipment which should work, especially during the military operations. According to current NATO reports, between 8 to 10 intrusion attacks have a high level of complexity. Moreover, other small-scale attacks have the Alliance IT networks as targets. Therefore, according to NATO reports there are over 2,500 significant cyber incidents annually that occur without the interruption of the services at the network level. Generally, low level cyber incidents, having either intrusion or spying purposes on the organisation systems are among the most frequent ones, while major military incidents occur seldom or they are not reported on a regular basis. Taking into account their characteristics, it could be said that cyber threats have a global character and the risks which are created by the virtual space are constantly increasing. The Internet infrastructure is essential for NATO member countries, taking into account the fact that companies and national economies are based on it. Therefore, the governments of the Alliance member countries are showing their concern towards the threats that come from the cyberspace.

Specialised literature in this field shows the present concerns regarding the semantic terminology of the cyberspace, in the sense that there are difficulties for approaching the subject in a clear and concise manner. It is worth noticing that the *cyber war* concept is used excessively, causing a lot of misunderstandings. This happens due to the fact that the virtual space is described inappropriately, by using a lot of metaphors or analogies with the battle field. This can be encountered not only in the media but also in the academic research and terminology in the political field. Considering that cyber threats are not entirely military, the Alliance tends to use proper terminology, without defining, up till now, an official version for the cyber field. Given the lack of a common agreement, ambiguous concepts such as *cyber attack* or *cyber war* must be defined precisely. Considering that NATO decisions are the results of negotiations, rhetoric becomes highly important. The present terminology and language are focused on threat representation and its assessment. Thus, NATO, having an important part in the global security environment, must express its position towards the general tendencies to overreaction and ambiguity when dealing with cyber semantics.

The present paper is developed focusing on three important NATO cyber security events and the manner in which the Alliance reacted to those challenges: the major cyber incidents from *Kosovo* (1999), *Estonia* (2007), as well as the outcomes of the *Stuxnet* (Iran, 2010) *malware* intrusion software. Due to the fact that the assessment of such threats at NATO level has changed significantly, the present article focuses on observing the complexity of cyber terminology and the manner in which it is used within the Alliance. By introducing scalability regarding the possible methods of coping with cyber conflicts, a solution is considered as referred to the manner in which NATO can find a semantic constant pattern for assessing prospective threats as well as for anticipating what kind of cyber attacks will be analysed by the Alliance.

One of NATO priorities is represented by the present and future threats to its members. A series of events have revealed the fact that cyber activities can influence prosperity, security and both national and transatlantic security. Having a clear image of the virtual space enables displaying, changing and/or deleting the existing information from the computers either at the individual and/or at the network levels, being highly difficult, sometimes even impossible to determine the actors of such actions. The main reason is that identities from the cyber environment can be easily hidden, enabling those responsible to remain anonymous.

There are mainly three different techniques that can be applied to cyber conflicts: *DoS (Denial of Service)*, *malware* and *hacking attacks.*

DoS refers to the premeditated attempts of making a server unavailable, by flooding it with a lot of traffic, which is created artificially within the network. The well-known version is *DDoS (Distributed Denial of Service)*, by which multiple systems and Internet connections often contribute to creating *botnets*, at the target computer level, having as expected outcome blocking the WEB and the servers. By contrast, *malware* uses different methods of clandestine intrusion, having the purpose of changing or deleting files. A common example of *malware* is the so-called virus, a code that can enter the existing applications, causing major damage, such as destroying the hard disk by compromising the information. In addition, *Worms* are specific kinds of viruses that are sent aggressively from one computer to another, being more independent.

❖ Cyber Semantics – terms and definitions

So far there has not been a common version regarding the proper definition of the hostile incidents that come from the cyberspace. Thus, there is no universal understanding upon the specific key concepts for the cyber field. Therefore, NATO does not agree any existent definition of them. Many times, in the official statements regarding cyber incidents, NATO representatives do not succeed in using coherent terminology. For instance, in the case of the cyber attack from Kosovo, the Alliance used simple references regarding the technical terminology and the consequences of its use, while *DoS* attacks (Estonia) were described as *"strategic bombings"*, by mentioning the strategic implications, too. *"Cyber-attack"* and *"cyber-defence"* have been used many times throughout the events, being regarded as anticipation of the upcoming 21st century security challenges. Within this framework, former NATO Secretary General, Jaap de Hoop Scheffer, emphasised on several occasions that *"cyberspace has become a kind of battle field in peace time"*. Such comments indicate the tendency in the official statements at military and defence levels to avoid using the concept of *"cyber war"*. However, the Estonian Minister of Defence, Jaak Aavicksoo, stated that: *"the cyber attacks against Estonia were real acts of cyber war and terrorism"*. Nevertheless, the rhetoric of war is quite problematic as representing conflict this way contributes to increasing the risk of non-military cyber incidents within the international armed conflicts. The reference to *Stuxnet* in NATO official releases showed that the organisation intensified its rhetoric by using military representations, in order to reflect the severe and unseen nature of the events. The official releases of the Alliance referred to the *"cyber attack against the operating system of the nuclear plant"*, *Stuxnet* being described as an *"offensive cyber weapon"*. Taking into account the existent terminology, *"cyber attack"* is the most frequently used term.

The linguistic representation of the cyber topic at NATO and member countries level is definitely influenced by the US assessment and explanation system. Thus, it is worth noticing the cyber semantics at a comprehensive level within the members of the Alliance, especially at that of the most powerful ones. On 11 October 2012, the US Defense Secretary, Leon Panetta, presented briefly the US point of view upon cyber security in a paradigmatic discourse. He presented demonstratively the cyberspace as *"a new field for carrying out the war"* and *"a battle field of the future"*. Panetta transferred two of the most traumatising events in the history of the USA into the cyber field; he not only predicted a *"cyber Pearl Harbor"*, but he also made reference to a *"prior 9/11 moment"*. Due to this perception of the threat, he concluded that *"the most important investment"* must be made *"in highly qualified cyber fighters"*. This language clearly highlights the intent of positioning the cyberspace within the military field and emphasises the rationale of military solutions, focusing on the need to ensure proper financial support.

The lack of a unitary military terminology in the cyber field contributes to the existence of unclear and inexact concepts, creating confusions in the debates regarding cyber conflicts. Different classifications have different significances and various consequences. For instance, in the discourse referring to *cyber crime*, the concept is placed within the police field, whereas *cyber war* signifies that it is an issue which must be handled by the military. Thus, the manner in which words are selected influences the political decisions and contributes to the need for clarifying the answer, regarding the manner in which *cyber threats* can be dealt with efficiently and the role the Alliance should play in this context.

This aspect has a crucial importance, due to the fact that the differences in assessing the threats can make the cooperation efforts more difficult at both national and international level.

Thus, the attempt to establish, within NATO, an accepted definition regarding the fundamental terminology specific to the cyber field becomes a priority, due to the fact that the issues connected to identifying the authors of the cyber attacks cannot be always established precisely. Notwithstanding, a certain distinction between different kinds of conflicts is made from the point of view of their nature and the actors involved, as well as of the intentions and the desired purposes. The following definitions represent the basis for the present and ongoing debates.

- ***Hacktivism and cyber vandalism***

The concept of *hacktivism* comprises the terms *hacking* and *activism*. It refers to the activity of independent persons and groups that exploit computers and computer networks by special *hacking* (*unauthorised access*) techniques, using the cyberspace as an environment for protests and promoting political purposes. The intent is represented by blocking the legitimate use of information, for instance, destroying the Web sites or interrupting the Web services. By contrast, cyber *vandalism* is motivated by the hackers' curiosity and self assurance of the professional characteristics, lacking in a political agenda.

- ***Cyber crime***

Cyber criminals use the cyberspace to their advantage for promoting illegal activities, which are sometimes carried out within an organisation. *Cyber crime* is motivated financially and it includes a wide range of crimes, such as: credit card forgery, identity theft and fund extortion, having as targets both individuals and companies.

- ***Cyber espionage***

A series of companies, states as well as institutions – through private hackers – spy on the targets, by using complex techniques (*cyber espionage*). Economic espionage must be looked at differently than either political or military espionage as the former deals with confidential information regarding the business and intellectual property of significant economic assets, whereas for the latter the main goal is access to information that is connected to the national security, strategic and military capabilities. Another potential objective is represented by testing the defence configurations of some targets belonging to the communications and information architecture.

- ***Cyber sabotage***

A distinction is needed between economic sabotage and political-military sabotage. Drawing a line between *cyber espionage* and *cyber sabotage* is not clear, because the same actors can be involved in the two kinds of activities. Both of them can operate in sequences, in the sense that *cyber sabotage* uses the advantages of the security breaches and the vulnerabilities identified by *cyber espionage*. The latter above-mentioned concept is directed towards the integrity and availability of either economic or political-military processes and the operation of the main IT systems, interrupting or even destroying equipment or information. Cyber sabotage, unlike hacktivism or cyber vandalism, affects the national security, remaining below the cyber war level.

- ***Cyber terrorism***

Terrorist groups or networks, such as individuals with radical views, might use the cyberspace for attracting the public attention to their requests, by systematically planning violent actions that cause the destruction of the critical infrastructure components. The possible outcomes of *cyber terrorism* attacks have the following purposes: plane crashes, polluting waters or interrupting the electric power supply. Cyber terrorism is more than an action that can be condemned, taking into account the victims and the material damage.

- ***Cyber war***

National armed forces, such as those financed by the government, respectively the state authorised militia, such as mercenaries, could use cyber techniques for causing damages or blocking the military capacities, the communication systems or the critical infrastructures of the enemy nations. Without damage or material losses, a *cyber conflict* cannot be viewed as a *cyber war*. Moreover, if the aggressor is not a state actor, war is out of question. According to the accepted terminology, an act of war must be instrumental and must involve the use of force for political purposes. This principle could be also applied to the cyberspace military conflicts.

Cyber war is an ambiguous and controversial term, requiring a detailed examination. In the light of these considerations, it could be stated that cyber war develops along with other military actions, being, in fact, a support capability. This means that reference to *cyber warfare* is more appropriate. As in the conventional military strategy, *tactical cyber warfare* must be looked at differently than *strategic cyber warfare*. From a tactical point of view, the cyber armed forces have the objective of reaching prominent positions on the battle field, by means of communications and information systems, facilitating kinetic attacks, for instance through entering and corrupting the leading data systems, utilising the means which are specific to cyber technologies. In other words, cyber capabilities facilitate traditional military operations, being at the same time means of reducing the number of vulnerabilities to the enemy equipment. On the other hand, when a belligerent attempts to obtain strategic advantage during a confrontation, the functional capabilities of the enemy become targets. For instance, the national critical infrastructures are attacked. It is worth noticing that both cyber war levels presented previously will play a significant role in prospective armed conflicts. By contrast, experts consider that a stand-alone cyber conflict which is independent from large-scale conflicts but has a high level of predictability for carrying out cyber attacks seems less likely for now. China, Russia, Israel, France, the UK and the USA have all the needed technologies for launching cyber attacks that can cause serious damage up to reaching the appropriate level for acts of war. Therefore, it is less likely that political leaders will authorise high level cyber attacks, similarly to taking decisions regarding launching missile attacks. The benefits of a cyber attack are hard to be estimated due to the existent risks. The outcomes can be uncertain and combatants may not have the needed skills for defending against complex cyber attacks. It is worth mentioning that sometimes the side effects of cyber weapons have an increased importance created by the media or by company advisors. Usually, cyber conflicts cannot be compared to violent military actions, if we consider the consequences of launching a nuclear missile, for instance. Therefore, the total capacity of resistance or countering a prospective threat cannot be undermined decisively. Notwithstanding, the cyber weapon issue represents a serious concern within NATO, focusing mainly on the defence strategy against cyber threats and taking into account the legal and ethical issues regarding the use of cyber instruments. Therefore, military and political decision-makers must pay special attention to the circumstances in which using cyber weapons can lead to benefits, outside the traditional battlefield.

The *cyber attack* concept must be given special attention because it has a variety of significances, depending on the security field. For diminishing the level of confusion and uncertainty in the military field, the *cyber attack* term should be used only for describing *cyber conflicts* that have a military characteristic. Their effects should be harmful to a significant extent (destructive, obvious and immediate) or corruptive (subtle or persistent). As a consequence, only the cases of *cyber sabotage*, *cyber terrorism* and *cyber war* should be identified as being *cyber attacks*.

It is highly important to define, at NATO level, the framework that authorises the use of force by means of *cyber technology*. The manual regarding the international law that can be applied to the cyber war, released by *NATO CCDCOE – Cooperative Cyber Defence Centre of Excellence in Tallinn* (without being a NATO directive), defines an attack, justifiable from the military point of view as being: *“a cyber operation, whether offensive or defensive, which is reasonably expected to cause injury or death to persons or damage or destruction of objects”*. The definition is characterised by the nature of the results, in the sense that, if a cyber operation is followed by significant destructive consequences, it is described as a *cyber attack* as well as a use of force. If the hostility of cyber activity produces only reasons of dissatisfaction it represents neither a *cyber attack* nor a use of force. Understanding this term is essential, taking into account that its assessment is part of further political decisions.

CYBER Conflict Development Scale

Previous analyses and assessments highlight that there is a general phenomenon of approaching the *cyber semantics*, which is sometimes characterised by exaggerations and non-differentiated patterns of language. For solving this issue, the paper presents in *figure 1* the above-mentioned types of cyber conflicts (*hacktivism, cyber vandalism*, *cyber crime, cyber espionage, cyber sabotage, cyber terrorism* and *cyber war*), taking into account two main features, namely their occurrence and the level of destruction or the severity of effects.

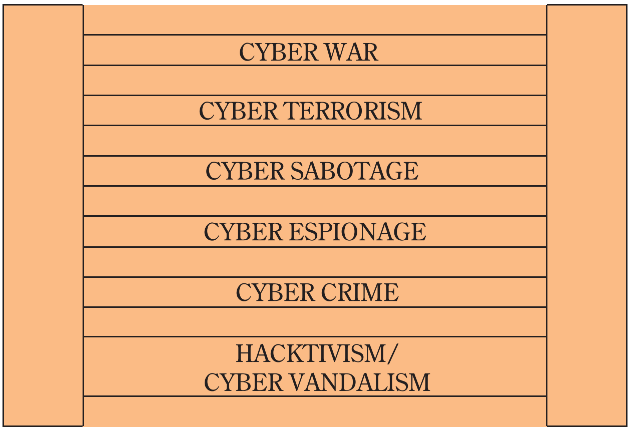


Figure 1: Cyber conflict development scale

According to this pattern, the dominant types of conflict are represented by hacktivism, cyber vandalism, cyber crime and cyber espionage. The former two have a limited security impact and do not influence the national interests, being irrelevant as far as NATO missions and mandate are concerned. They influence only the standard strategic level of training and are part of the *CIRC – Computer Incident Response Capability* security procedures at NATO level. These kinds of conflicts are crimes against the national laws, and, for their punishment, the authorised civilian institutions are responsible.

Cyber espionage holds a special place, the indirect damages having serious results. On the one hand, the transition towards cyber sabotage is fluid, and, on the other hand, the information that is obtained could be used for cyber terrorism and/or cyber war. Therefore, these kinds of activities have a great impact upon the national security. NATO has to give special priority to counteracting cyber espionage. Implementing such developed methods of security is mandatory for the operational and classified networks of the Alliance. International laws do not ban cyber espionage, being considered, similarly to conventional espionage, a crime which should be punished according to national laws. Moreover, the responsibility for combating cyber espionage actions is assigned to the agencies which are specialised in counter espionage activities.

The cyber conflict development scale shows that cyber espionage, cyber terrorism and cyber war occur occasionally. There are few examples of cyber attacks that caused physical damage and destruction in the long run as it happened with *Stuxnet*, the only example of cyber interstate attack of this kind. It is worth noting that no cyber war has been carried out so far. Nevertheless, NATO must give special attention to these three kinds of cyber conflicts, because they include a high potential that can cause serious damages, at both national and international level. Therefore, the ministries of defence, the national armed forces and the Alliance have a significant role in dealing with these kinds of threats. Within this framework, *figure 2* presents the types of cyber conflicts, taking into account the security impact level.

CATEGORIES OF CYBER ACTIVITIES	SECURITY IMPACT LEVEL		
		LOW	HIGH
	THEFT	HACKTIVISM CYBER CRIME CYBER VANDALISM	CYBER ESPIONAGE
	INTERRUPTION	HACKTIVISM CYBER CRIME CYBER VANDALISM	CYBER SABOTAGE CYBER TERRORISM CYBER WAR

Figure 2: Cyber conflicts according to the security impact level

As far as the military dimension of the cyber threat is concerned, NATO is interested in two directions. First, cyber attacks can be relevant for the Article IV of the Washington Treaty. As a political-military Alliance, NATO consults with member countries whenever *"the territorial integrity, the political independence or security of any of the Parties is threatened"*. Cyber security is important because it facilitates procedures of consultancy and assistance, if cyber attacks are under the level of an armed attack. Second, cyber attacks could be described as armed attacks, when the provisions of the Article V are met. It is according to the statement that *"an armed attack against one or more of them (member states) in Europe or North America shall be considered an attack against them all"*.

NATO Options in the Cyberspace

As for the challenges created by the virtual space, NATO must play a significant role, even though this fact will intensify further debates. All the important armies are getting ready in the cyber field, regarding both analytical aspects and cutting-edge equipment. Cyber capabilities will be certainly used in any future military conflict. According to the experts in the field, it is less likely to carry out a devastating cyber war. However, it is likely to conduct a cyber war at strategic and tactical level, within the traditional war context. NATO mission as a political-military alliance is defensive and this aspect can be also applied at the cyber security level. Nevertheless, NATO must take into account the cyber threats from a military perspective, too. It does not necessarily mean changing all the cyber threats from non-military to military, as it is the case of several low-level impact cyber intrusions NATO is currently dealing with.

For proper risk analysis, the Alliance must consider the potential and the motivation of the prospective opponents. The essential question must refer to: *"Who is interested in attacking the NATO cyberspace or the one of its member states and who has the capability of accomplishing it?"* and less to: *"Where is NATO vulnerable?"* For the military, planning the confrontation with the worst scenarios is a legitimate course of action. Nevertheless, using multiple resources within the framework of few possibilities of producing catastrophic incidents makes sense neither strategically nor financially. A conclusion is definitely clear in this context: the most important NATO task is the ongoing training in the field of cyber technology and semantics.

❖ Securing the IT infrastructure

Taking into account the nature of cyber threats, the actions for technical security represent a priority for strengthening the cyber defence elements. These actions should comprise NATO administrative and operational systems, because most of the risks are encountered at their level. Moreover, *vetting* procedures can be used for preventing inside attacks along with *baiting* techniques.

It is less likely that these cyber intrusions will be avoided completely, but developing capacities for reducing their effects becomes essential. The systems should have the rapid recovery ability and, if needed, they should resist under such attacks within the military conflict framework.

NATO key communications systems are interconnected unavoidably and the temporary unavailability of one is extended to the others, too. The member states are responsible for their own cyber security as well as for implementing preventive protection actions. However, for securing these crucial systems, NATO should support the Allies, strengthening their cyber defence capabilities regarding the protection of civil and military infrastructures.

❖ **Proper semantic terminology**

Apart from technical actions, the proper semantic representation of cyber threats is an essential requirement for defining the concept of cyber security. Within a virtual secure space, a vague concept as well as a careless use of the *cyber war* and *cyber attack* terms can become dangerous. In our opinion, NATO should increase the efforts for classifying cyber conflicts and for explaining the cyber terminology that could ensure better information for the Alliance and for the member countries. Within this framework, common definitions, similar to the presentation described above, and a reference scale for assessing the level of conflict development are needed.

The pattern of conflict scalability suggests that cyber sabotage, cyber terrorism and cyber war are threats relevant for NATO, as a defensive alliance, without considering lowering this level. Cyber crime and cyber espionage must not be mistaken for the cyber war. This final term could be used only for describing a major cyber conflict in which more states are involved, having an impact on the real world. Within the context of an international defence organisation, the term of *cyber attack* could be used only for the *cyber activities* that harm the people and the property.

Using military specific language – including the excessive use of the term *cyber war* – creates the premises for a feeling of fear towards the cyber capacities of the enemies. An open rhetoric of discouragement could also increase tensions, causing an escalation into the virtual space militarisation and the cyber conflict, rather than avoiding them. A clear delimitation of the definitions could mitigate the risks substantially. At the same time, a semantic terminology which is well developed will contribute to preventing the escalation of non-military conflicts into armed conflicts. Within this framework, NATO could contribute to reducing the rhetoric of tension, simultaneously with maintaining an increased attention to cyber threats. NATO has a great potential for debate and for implementing the cyber security measures along with the member countries and other partners. The proper choice of language will promote an environment for urgent establishment of necessary norms and of international agreements connected to the virtual space management. The present grey area of the international legislation must focus on clearly defining the cyber activity types that are allowed to (non)-state actors.

Within NATO, the military dimension of cyber threats should be defined in a clear and unanimously accepted manner. The nature and the extent of damage that could lead to putting into practice the Article V should be clearly explained for cyber conflicts. In the end, it would be a political decision whether or not a certain cyber conflict is assessed as cyber war. For safety reasons, this decision should have a precise linguistic basis.

NATO could promote as a global priority, regarding the cyber security issues, the objective of diminishing the threats coming from the virtual space, by using the most effective political-military mechanisms. Therefore, cyber semantics is essential in the light of the initiatives regarding diminishing the development of prospective conflicts launched from the cyberspace.

NATO should also state its position towards the worst cyber scenarios, promoted based on imprecise assessments of threats, on sensational and dramatic rhetoric, even though they belong to the mass-media or to a multitude of decision-making factors.

BILBIOGRAPHY

1. Myriam Dunn Caveltry, *The Militarization of Cyber Security as a Source of Global Tension*, Ed. Daniel Mockli, Zurich, 2012.

2. James A. Lewis, *Conflict and Negotiation in Cyberspace*, 2013, see http://csis.org/files/publication/130208.

3. Bruce Schneider, *When Does Cyber Spying Become a Cyber Attack*, Atlantic, Berlin, 2014.

4. ***, Answer to Your Questions, 2011, see http://atlanticcommunity.org/index.php/Open_Think_Thank_Article.

5. ***, *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation* adopted by Heads of State an Government, Lisbon, 2010.

6. ***, *Glossary of Terms and Definitions*, see http://www.fas.org/irp/doddir/other/NATO2008.pdf.

7. ***, *Talinn Manual on the International Law Applicable to Cyber Warfare*, Michael N. Schmitt, Tallinn, 2013.

CYBERSPACE CARTOGRAPHY

BEng Alexandra DINULESCU
BEng Gheorghe URSULEAN

The information technology development and its use in everyday life have led to a mainly virtual artificial environment, called cyberspace. According to one of the widely accepted definitions, cyberspace comprises all the elements that store, transport and process information, as well as all the procedures associated to them. Apart from the fact that the processes that are carried out within this environment have changed the lifestyle drastically, cyberspace is also considered a strategic field. Moreover, it is a place where both offensive and defensive cyber operations able to reach the extent of cyber wars can occur. Taking decisions related to cyber defence requires maps for the area of responsibility or the locations where operations could take place. Although some key features belonging to traditional operational maps are preserved, cyber maps are more complex and have more dynamic representations. The article presents the methods and tendencies in cyberspace cartography.

Keywords: *cyberspace; map; cartography; Internet; technology*

I. Historical Milestones of Cartography

Cartography represents the art, science and technology of creating maps. It also refers to the maps role as scientific documents and art works. The *map*, the key element of cartography is a graphical representation or a scale pattern of the location coordinates, facilitating understanding of concepts, conditions, processes or events within the context, being, at the same time, a universal means of communication. The history of cartography began when the first indications of land navigation appeared, being communicated either orally or on the sand. Since then, people have tried to represent as well as possible the manner in which the surrounding environment could be understood. The oldest examples of maps come from the Palaeolithic Age, about 25,000 BC. They are rudimentary representations of both geographic and topographic characteristics such as: hills, rivers and places to live. Primitive maps included representations of local tracts of land and they were mainly used for depicting hunting places or areas with food and water. Around 6200 BC the Egyptians carried out field measurements and represented them graphically in order to be able to rebuild the local borders after the floods.

BEng Alexandra Dinulescu, BEng Gheorghe Ursulean – the Ministry of National Defence.

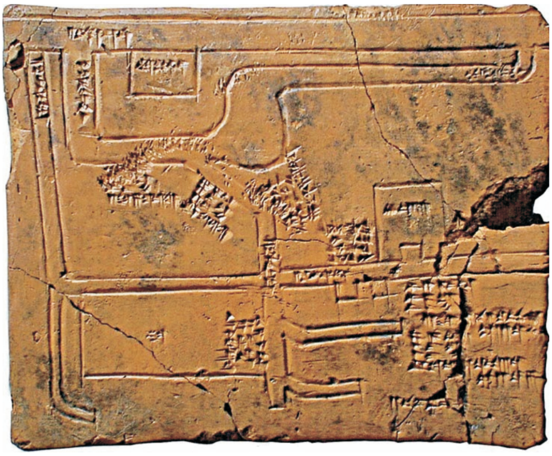


Figure 1: Babylonian Map, irrigation canals 1684 BC

The first map of the world was created by the Babylonians in the 6th century BC and it showed Babylon surrounded by a circular tract of land and other cities, reflecting the religious beliefs of the time. Since the carvings inside the caves and the ancient maps of Babylon, Greece or Asia people have created maps and basic tools to better understand the world and to be easily guided through it.

The diversity of commercial routes and the need for discovering and conquering new lands were good reasons that determined people to carry out expeditions along the seas and oceans. Sailing required skills and bravery, and navigational charts represented useful ways that facilitated commercial sailing, transport and conquest of lands, with the help of their clear and precise indications[1]. Navigational charts have improved over the years. Starting with the Mediterranean harbours at the end of the 13th century and the first atlas that included navigational charts, in 1584, at the beginning of the 17th century, the graphical representation of the oceans and shore lines became a strategic naval and commercial requirement. Nowadays, the advantages brought by technology improve the hydrographic studies and ensure the design of precise and complex navigational charts.

At the beginning of the 1900s, the Wright brothers carried out the first flights marking, this way, the beginning of the aviation domain. Direct visibility represented, at that time, the main tool that enabled navigation. An aircraft could carry out only short distance flights in clear sky weather conditions, and pilots used the transport routes and borders, having to fly at a low altitude above the railway

[1] John Blake, *The Sea Chart: The Illustrated History of Nautical Maps and Navigational Charts*, 2009, see http://gpspathfinder.work/racks/T/The-Sea-Chart-The-Illustrated-History-Of-Nautical-Maps-And-Navigational-Charts-Paperback.pdf

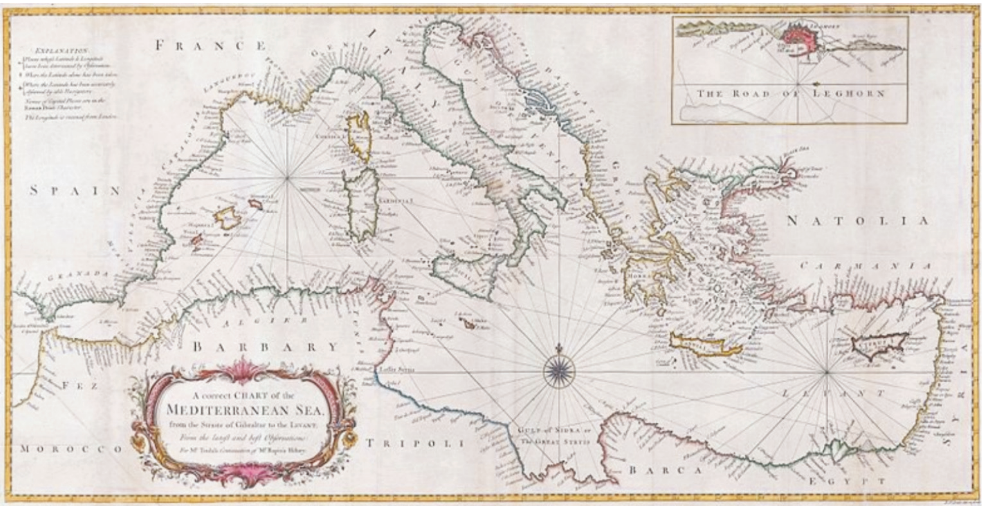


Figure 2: Map for navigation in the Mediterranean Sea, 1745

tracks because of the low visibility conditions. The first pilots started to use personal notes that enabled them to navigate. Starting with the first navigation manual *"Jepp Charts*", in 1930, which included Captain Jeppesen's personal observations regarding landing places, obstacles and the heights of the hills as well as other significant route characteristics and up to the present modern navigation charts that are constantly monitored, improved and updated by the International Civil Aviation Organisation – ICAO, the air charts have been continuously improved in order to keep pace with current technological requirements and developments.

The present air traffic maps are updated in real time. The update frequency of positions is in seconds and the coverage is global. A multitude of air traffic dynamic maps are available on the Internet. In our opinion, there are two representative sites[2] in this regard. Such a map is presented in *figure 3*.

These maps are usually interactive, with context options and different possibilities for instant and synchronised reports of statistics and selected relevant events. For instance, clicking the symbol of a certain aircraft can start the display of detailed data of the flight in a separate window. In addition, philtres can be set in order to highlight certain flights or the ones that do not follow specific flight corridors or charts.

Almost simultaneously with guidance and navigation maps, which have important roles, but are oriented mainly to symbolic representations of an area of interest, military maps appeared using the above-mentioned categories only as background for representing the own forces or those of the enemies, field representations

[2] See http://www.flightradar24.com and http://planefinder.net

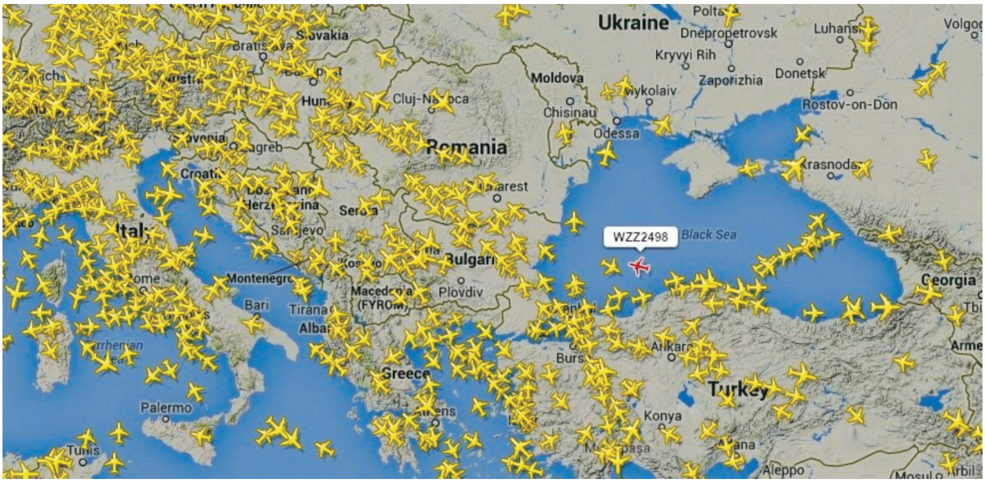


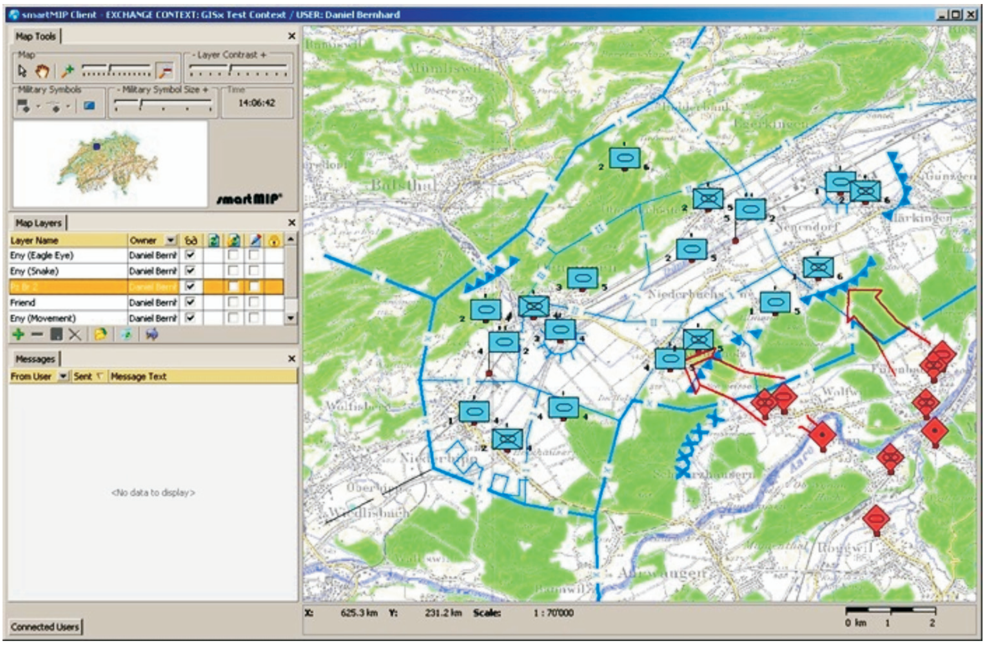
Figure 3: Picture of an air traffic dynamics map[3]

that have tactical, operational and strategic utility, concepts and either the own and the enemy intentions, outcomes and prognoses. In other words, the military map combines in a unique image the field elements with the situational and conceptual ones along with the commander's decision. The accomplishment of a mission depends on the value of the commander's decision, which, apart from his training and thinking, is influenced by the quality and the clarity of the situational map.

The operational map has an important role in communicating to subordinates both decisions and courses of action. The fact that the map and the excerpts from the operational map are attached to the order of action enables sending a great part of information rapidly from the decision-makers to the ones that conduct the actions, diminishing the chances for misinterpretations or confusions that could have serious consequences in the theatre of operations.

The military operational map can be interpreted as the entire operation radiography. Therefore, apart from the central role it has throughout the mission, the military operational map is very important for post-conflict analysis and for training officers and commanders. Many military exercises are carried out only on the map, being also based on simulations or military games. Along with using technology for the military map and generalising the use of *Geographic Information System – GIS* capabilities in military headquarters, there is the possibility of testing and comparing certain operational scenarios throughout the decision-making process.

[3] See http://www.flightradar24.com/



smartMIP Client - EXCHANGE CONTEXT: GISx Test Context / USER: Daniel Bernhard

Map Layers

Layer Name	Owner					
Eny (Eagle Eye)	Daniel Bernh	☑		□	□	
Eny (Snake)	Daniel Bernh	☑		□	□	
Pz Br 2	Daniel Bernh	☑		□	□	
Friend	Daniel Bernh	☑		□	□	
Eny (Movement)	Daniel Bernh	☑		□	□	

Messages

From User	Sent	Message Text

<No data to display>

X: 625.3 km Y: 231.2 km Scale: 1 : 70'000

Figure 4: GIS operational military map

II. The Use of Cyber Maps

Throughout the years, many definitions for the cyberspace have been proposed, taking into account the different perspectives of the sources. *The US Department of Defence Strategy for Operating in Cyberspace* presents cyberspace as a domain characterised by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructure[4]. In addition, the first strategic initiative presented in the above-mentioned document shows that the USA will treat cyberspace as an operational field. Therefore, it will equip, train and empower the Department of Defence to protect the national interests in this field, as it does in the land, maritime, air and cosmic space.

In order to indicate the cyberspace dynamics, this could be defined as a time-dependent set of interconnected information systems and the human users that interact with these systems[5]. The impressive dynamics that characterise this environment represent the basis for establishing a new objective

[4] Department of Defense, *The National Military Strategy for Cyberspace Operations*, Washington, DC: Department of Defense, December 2006, see http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf

[5] Rain Ottis and Peeter Lorents, *Cyberspace: Definitions and Implications*, Proceedings of the 5th International Conference on Information Warfare and Security, Ohio, USA, 2010, pp. 267-270.

in the traditional cartography: cyberspace cartography. Cartography is a manner of externalising the concepts from the cyberspace, having the purpose of giving them significance, making them comprehensible and easy to be used, ensuring, at the same time, a context for every concept and its relations with others. It also shows important aspects connected to those that control the infrastructure or have access to the cyberspace and the manner in which they can be observed. Different thematic maps have been created in the attempt of defining the complex space geometries of the cyberspace, the New World of the 21st century. Several maps and visualising elements, similar to the maps created until now, are focused mainly on locating the elements of infrastructure, determining the data traffic and the statistics regarding the users, the Internet services from the market, ensuring the efficient management of Internet resources, improving Web searches and identifying potential access gates within the cyberspace.

The progress in the information technology field within the present social, political and military context has changed the cyberspace into a real war zone where the countries of the world fight for digital supremacy in a new and almost unpredictable theatre of operations. Cyber operations represent a significant chapter in safeguarding national sovereignty and projecting power. The capacity to successfully carry out missions and to ensure strategic advantage in the cyberspace is greatly influenced by the ability to understand, represent and analyse this complex territory which has a dynamic evolution. One of Sun Tzu principles from *The Art of War*: *"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself, but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle"* is entirely applicable to the cyberspace.

From the cyber strategic espionage campaigns such as: *Moonlight Maze*, *Titan Rain* or *Dragonfly* to the destructive cyber military attacks in Estonia, Georgia or Iran, people and international conflicts pass to another phase of history. On this vague battle field, represented by the cyberspace, fights are carried out with bites rather than bullets, *malware* instead of troops and *botnets* instead of bombs. Knowing in real time the status of own resources and capabilities as well as the enemy actions and intentions is vital for defending and promoting the national interest, requiring attention and resources, needed for cartography and proper monitoring of the areas of responsibility in the cyberspace.

Figure 5: CO 624 Lackland, one of the dozens of American bases specialised in cyberspace operations

III. Cyber Map Characteristics

1. The nature of the described elements. Unlike traditional maps that include symbols of other elements, cyber maps operate with abstract elements, some of them virtual. According to the definition given in the first part of the article, the ways of communication, either physical or virtual, electromagnetic ones included, are part of the cyberspace. Storing devices, structures and data bases, data floods, applicable systems, authorising and security elements, backup and disaster/recovery systems are all parts of the cyberspace. Some elements are protected by codes, firewalls, demilitarised zones – DMZ and access management. All these contribute to making cartography of the interest zones within the cyberspace quite challenging.

2. Limitations. Cyber maps have quite fast dynamics. Entire parts of the cyberspace can be multiplied almost instantaneously.

3. Novelty of the field. Cyberspace passed the critical barrier for being dealt with as a new business field. However, the challenge began in early 21st century. Moreover, the migration of resources and processes in the *New World of the 21st Century* is currently changing. Thus, acquiring expertise in the field of cyberspace cartography is limited.

4. Complexity. It is estimated that nowadays almost one third of the world population accesses the online environment. The increase in the number of users, the devices connected to a network and the services that include a significant

Figure 6: Representation of actors and fields in the information technology

amount of data have led to a greater need for a bandwidth. *Cisco VNI*[6] provides the most trustworthy assessments. In 2013, there were 111,366 million Internet secure servers, over 670 million Internet subscribers, and 38.13% of the world population used the Internet. According to *Cisco VNI* the global IP traffic will exceed the zeta byte limit in 2016 reaching up to 1.1 zeta bytes a year, whereas, in 2018, it is estimated that it will reach 1.6 zeta bytes a year. On the night of 16/17 September 2014, there were more than 1 billion websites and 3 billion users.

IV. Practical Options for Cyberspace Cartography

1. The Atlas of Cyberspace, written by Martin Dodge and Rob Kitchin is the first complete work that explores the spatial and visual nature of the cyberspace and its infrastructure. It resulted after more than 30 years of research, comprising complex and various areas of the cyberspace. Martin Dodge and Rob Kitchin examined the manners for using cartography on the Internet infrastructure and data traffic, innovations in interactive web cartography, maps of conversations and communications in the field.

2. The modern version of *The Atlas of Cyberspace* is *The RIPE Atlas*, a global network of probes that measure Internet access and connectivity, offering a real time image of the Internet. Any individual that connects an authorised probe adds, at the same time, a new probe to the *RIPE Atlas* that can be used for carrying out measurements upon the own network.

3. NORSE Company offers online maps of the Internet, updated in real time, which comprise information regarding the attacks that are initiated in different parts

[6] See Cisco Visual Networking Index

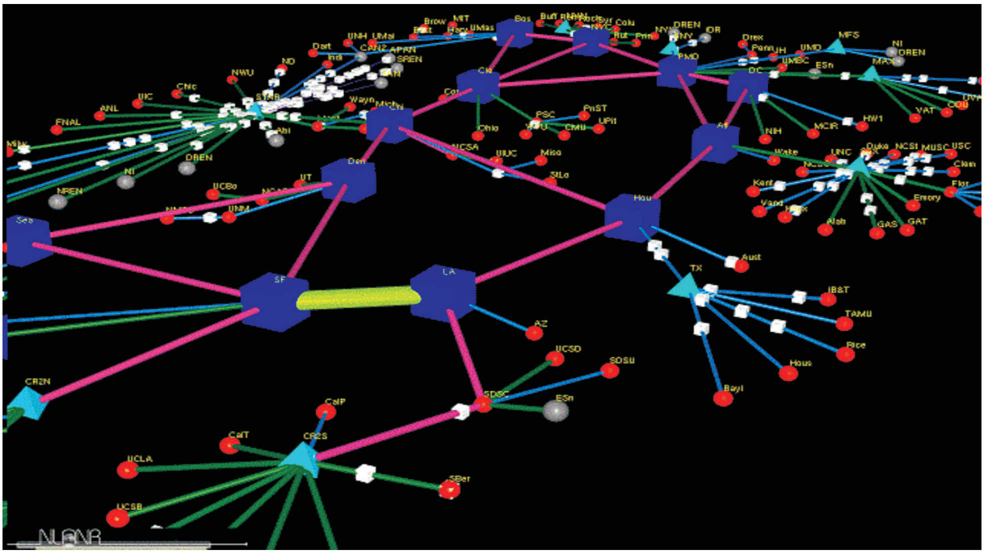
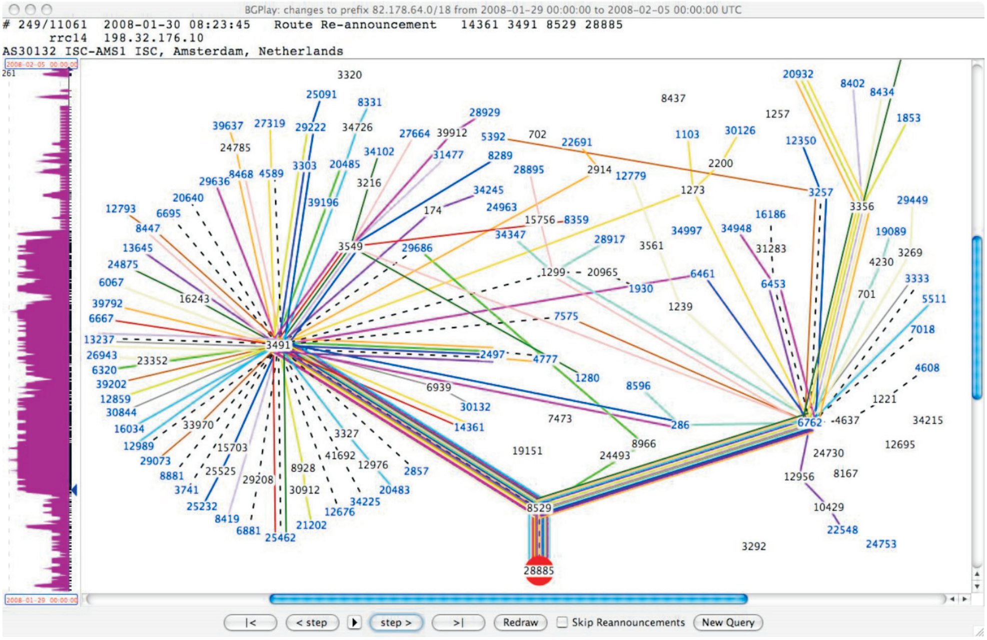


Figure 7: Topological representation version[7]


BGPlay: changes to prefix 82.178.64.0/18 from 2008-01-29 00:00:00 to 2008-02-05 00:00:00 UTC

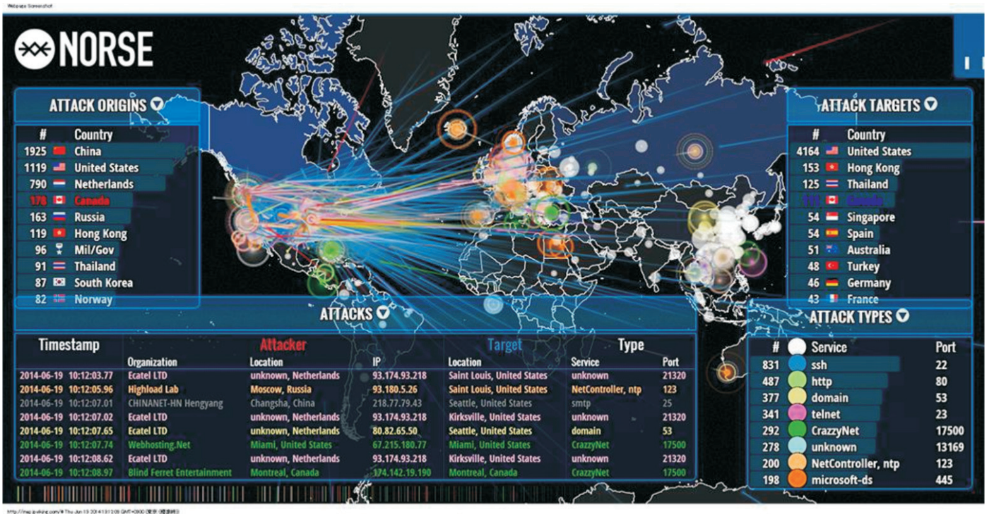
```
# 249/11061  2008-01-30 08:23:45   Route Re-announcement   14361 3491 8529 28885
       rrc14  198.32.176.10
AS30132 ISC-AMS1 ISC, Amsterdam, Netherlands
```

Figure 8: A RIPE version[8]

of the world, the time and the organisers of the attacks, the attackers' IPs and locations as well as regarding the targets, the services or entrances that are under attack.

[7] See http://www.atlasofcyberspace.com/

[8] See http://www.ripe.net



NORSE

ATTACK ORIGINS

#	Country
1925	China
1119	United States
790	Netherlands
178	Canada
163	Russia
119	Hong Kong
96	Mil/Gov
91	Thailand
87	South Korea
82	Norway

ATTACK TARGETS

#	Country
4164	United States
153	Hong Kong
125	Thailand
111	Canada
54	Singapore
54	Spain
51	Australia
48	Turkey
46	Germany
43	France

ATTACKS

Timestamp	Attacker			Target	Type	
	Organization	Location	IP	Location	Service	Port
2014-06-19 10:12:03.77	Ecatel LTD	unknown, Netherlands	93.174.93.218	Saint Louis, United States	unknown	21320
2014-06-19 10:12:05.96	Highload Lab	Moscow, Russia	93.180.5.26	Saint Louis, United States	NetController, ntp	123
2014-06-19 10:12:07.01	CHINANET-HN Hengyang	Changsha, China	218.77.79.43	Seattle, United States	smtp	25
2014-06-19 10:12:07.02	Ecatel LTD	unknown, Netherlands	93.174.93.218	Kirksville, United States	unknown	21320
2014-06-19 10:12:07.65	Ecatel LTD	unknown, Netherlands	80.82.65.50	Seattle, United States	domain	53
2014-06-19 10:12:07.74	Webhosting.Net	Miami, United States	67.215.180.77	Miami, United States	CrazzyNet	17500
2014-06-19 10:12:08.62	Ecatel LTD	unknown, Netherlands	93.174.93.218	Kirksville, United States	unknown	21320
2014-06-19 10:12:08.97	Blind Ferret Entertainment	Montreal, Canada	174.142.19.190	Montreal, Canada	CrazzyNet	17500

ATTACK TYPES

#	Service	Port
831	ssh	22
487	http	80
377	domain	53
341	telnet	23
292	CrazzyNet	17500
278	unknown	13169
200	NetController, ntp	123
198	microsoft-ds	445

Figure 9: Static capture[9]

4. *Kaspersky Company* is interested in promoting the security solutions that it produces. It has also designed and published an online interactive map that offers information in real time of the cyber attacks at global level. The map highlights a series of principles that are characteristic to cyberspace cartography.

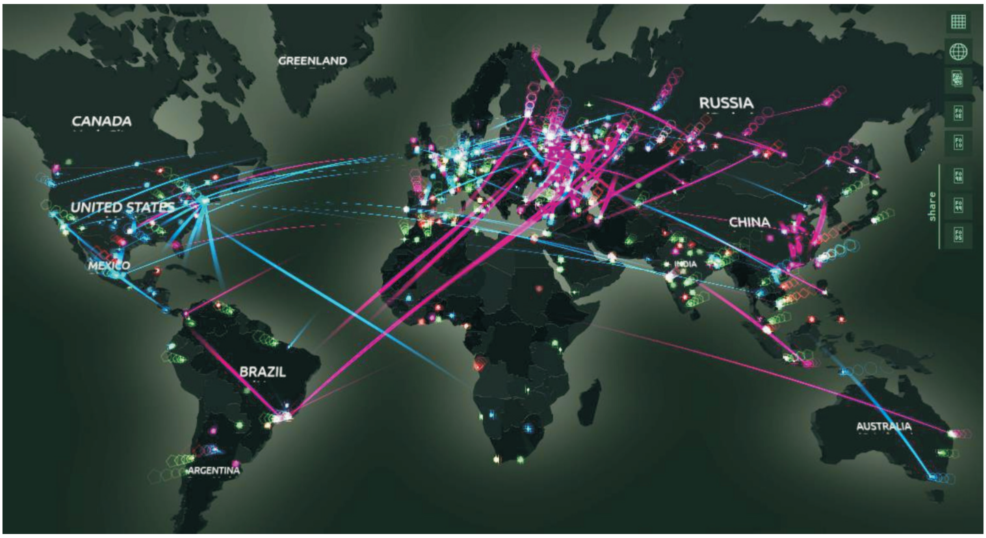


Figure 10: Static capture[10]

[9] See www.map.ipviking.com

[10] See http://cybermap.kaspersky.com/

5. *Visualising the links between entities.* It could be said that representing the entire cyberspace by following the pattern *The Map of the New World* is difficult to achieve and use. The most frequent requirements in cyberspace cartography are for creating thematic, specialised and selected maps, according to the area of interest and responsibility.

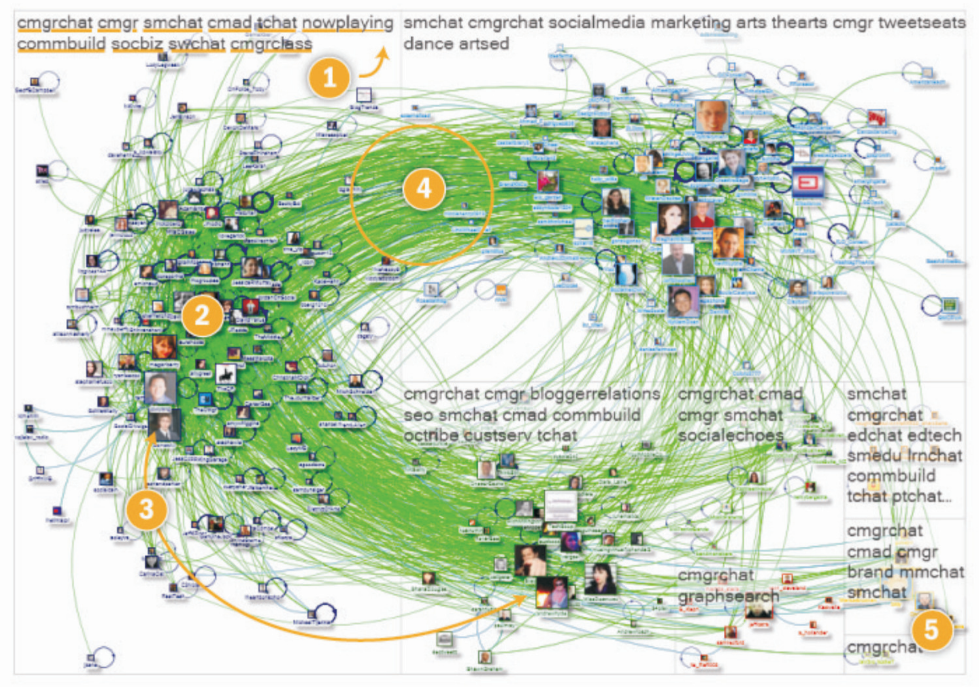

cmgrchat cmgr smchat cmad tchat nowplaying commbuild socbiz swchat cmgrclass
smchat cmgrchat socialmedia marketing arts thearts cmgr tweetseats dance artsed
1
4
2
3
cmgrchat cmgr bloggerrelations seo smchat cmad commbuild octribe custserv tchat
cmgrchat cmad cmgr smchat socialechoes
smchat cmgrchat edchat edtech smedu lrnchat commbuild tchat ptchat...
cmgrchat cmad cmgr brand mmchat smchat
cmgrchat graphsearch
5
cmgrchat

Figure 11: An example of a relation diagram within a social network

V. Tendencies and Challenges in Cyberspace Cartography

Maps are powerful means of selective communication of the messages. This is due to the fact that the map is mainly a process of development, including subjective decisions. The elements that are included or excluded on/from the map are the symbols and the messages that are to be communicated. In other words, maps reflect the cultural, historical and political context of the one that creates the map. Therefore, a map is not entirely objective and it is created in order to offer a certain image to the receiver of the message. Mark Monmonier in his book called *How to Lie with Maps* stated that: *"maps, like speeches or paintings are authored collections of information and also are subject to distorsions arising from ignorance, greed, ideological blindness or malice"*[11].

[11] Mark Monmonier, *How to Lie with Maps*, the University of Chicago Press, 1991, p. 2.

In order to illustrate the significant relations from an *n-dimensional* to a *bidimensional* space of a paper or a display, a map must distort the reality. Being a chart, the map uses symbols which, many times, are greater than the presented characteristics. In order to avoid hiding critical information in the multitude of details, the map must present a selective and incomplete view of reality. There is no such way of avoiding the cartographic paradox: in order to convey a useful and true image, little white lies are needed. The manner in which a person uses the information can change the map into a way of manipulating public opinion. The persuasion objectives are connected to national pride, strategic locations, attack vectors, defence means, influence groups, regional imbalance and other aspects connected to the cyberspace. A specialist in persuasion changes the message by means of maps, emphasising certain characteristics and leaving out contradictory information, along with adding a symbolic part[12]. Cyberspace maps represent important persuasion tools. They may be created in order to emphasise only certain aspects, presented depending on the objective. This is due to the fact that a map is not created in either cultural or political vacuum, being the outcome of individual ideas. To better understand the information displayed on the map, one must consider the local and global context in which the map is designed and used.

Among the numerous thematic maps created in order to visualise the cyber field there are maps that present certain characteristics such as: the number of Internet users, *Facebook* accounts, phone subscribers, the frequency of cyber attacks typical for every country. This information is an important tool for persuasion and misleading. When maps are used in order to display statistical data, the one that creates the map must present the data as accurately as possible. The purpose of data cartography is to generalise the data in order to facilitate the identification of the space coordinates. However, by generalising and simplifying data, some distributions can be easily hidden. The present technological level enables combining the surveillance means or those referring to the geospatial data bases and other *GIS* tools in order to produce maps that present different statistics in real time. Monitoring, identifying and obtaining statistical data that are the bases for these maps are prone to laws and regulations regarding the cyberspace, being essential in the discussions concerning the political groups. Therefore, the state establishes the political objectives, which are reached by creating different statistics through maps.

There are many misleading techniques which are known in the cyberspace. However, this aspect started being thoroughly checked only recently. Using *honeypot* systems or simple techniques such as inserting false information in the data stream,

[12] *Ibidem.*

false delays in the transfer of data and unreal error messages, the true image of the cyber zone is hidden so that it can be protected. Therefore, the attacker will initialise its actions starting from an incorrect image of the target. Maps can be good or bad depending on the owner, the user, the purpose, and the way they are used.

Users must consider that no matter how realistic maps may seem, they are just simple representations and they are vulnerable because of both the elements they display and those they leave out.

Conclusions

The chances for ensuring success in the security area of responsibility or in carrying out either defensive or offensive operations depend on the capacity of providing decision-makers with relevant information in real time. Therefore, the value of the decision depends not only on the commander's training, experience and thinking, but also on the quality of the operational map, which displays clearly and suggestively both the own and the enemy resources, the key tactical, operational and strategic elements, as well as simulations for the most probable courses of action. In other words, to defend own interests in the cyberspace and to simultaneously counteract hostile intentions, we consider that it is necessary to build the proper capabilities needed for cyberspace cartography and suggestive display of operational maps in areas of interest and responsibility in real time.

Selective Bibliography

1. Deborah Bodeau, Richard Graubart and William Heinbockel, *Mapping the Cyber Terrain*, MITRE, November 2013, see http://www.mitre.org/sites/default/files/publications/mapping-cyber-terrain-13-4175.pdf.

2. Gheorghe Ursulean, *Dezvoltări în spaţiul cibernetic. Provocări şi oportunităţi pentru serviciile de informaţii*, Defence Intelligence Directorate Symposium, November 2011.

3. Gheorghe Ursulean, *Colonizarea spaţiului cibernetic*, in *INFOSFERA*, no. 1/2012, pp. 62-71.

4. ***, Department of Defense – DOD, *Strategy for Operating in Cyberspace*, 2011, see www.defense.gov/news/d20110714cyber.pdf.

5. ***, *Strategia de securitate cibernetică a României*, 2013, see http://www.presidency.ro/static/ordine/SNAp/SNAp.pdf.

ADVANCED PERSISTENT CYBER THREATS ADDRESSED TO MILITARY CIS

Major BEng Georgiana GULIMAN
Captain BEng Alin-Marian PUNCIOIU

The organisations with responsibilities in the field of cyber security develop analytical platforms to investigate the mode of action of advanced persistent cyber threats to counteract these types of attacks. The main course of action is the implementation of scenarios such as "what would happen if ...". They allow for cloning and installing the security levels available to the organisation in secure environments where the access to information is only presumptive, thus deducing the vulnerabilities that can be exploited and analysing the possible consequences of a cyber attack on own infrastructure. The authors consider that, following the analysis of the results of an attack on the environment isolated and cloned for this purpose, security products able to integrate into the organisation infrastructure can be created, installed and tested.

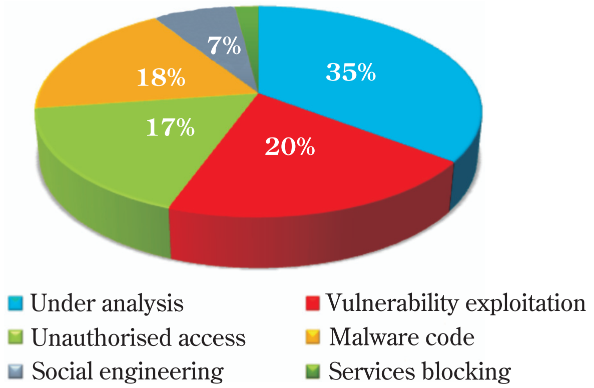
***Keywords**: cyber espionage; confidential information; national security; level of expertise*

Presently, states are exposed to cyber attack risks that may affect their physical or informational actives, their international actions or public image. Such attacks might be carried out for the purpose of deception or electronic espionage in order to get global competitive advantage, clandestine change of sensitive data within the theatres of operations and destruction or blockage of a country's critical infrastructure, such as energy, water, fuel, communications or commercial assets, essential to the society and economy functioning.

The sources of cyber threats are various: hackers, frustrated people, criminal organisations, extremist political groups, fanatic religious movements, hostile intelligence services, terrorist groups. *Verizon* 2014 data breach investigations report indicates that 95% of the attackers are foreign agents, activist groups, 4% internal employees/staff, and less than 1% business partners.

Militarily, these attacks might pursue sabotage, subversion, espionage, terrorism or organised crime, being materialised in data exfiltration, hindering mission development, inducing certain inconsistencies into the command-control systems (CC2) used in military operations etc.

Major BEng Georgiana Guliman, Captain BEng Alin-Marian Puncioiu – the Ministry of National Defence.



Among cyber attack methods, the following can be mentioned: vulnerability exploitation, acquiring unauthorised access, intelligence collection and alteration, services blocking or interrupting, introducing harmful codes, social engineering.

Cyber Threats

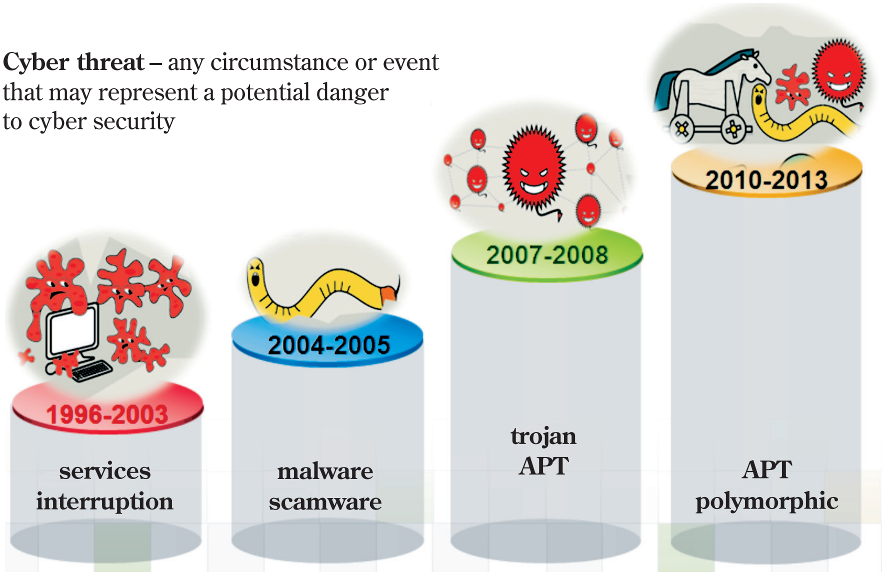
The development of cyber threats has been spectacular. *“Prior to 2000, if to make a comparison with Biology, viruses were conceived to make a lot of noise also because the authors wanted to become famous, to show their power. During 2000 to 2006, we witnessed ample attacks, on global scale, that could reach from one side of the planet to another in just minutes (…). After 2006, we witnessed again a change if you only consider that subsequent to Conficker up to the present, that is since 2008, we have not had another global virus. Therefore attacks have been conceived to strike only certain organisations. It is like a digital mosquito attempting to penetrate, without being noticed, the organisation’s defence systems and then lie inside in order to suck the blood, which is to steal the data. Ideally, the mosquito should be identified neither when it lies and observes, nor when it leaves, this is what the attackers want”*, says *Symantec* manager.

During 1996-2003, cyber attacks were aimed at interrupting/blocking the services using viruses, worms and *Distributed Denial of Service – DDoS* attacks.

During 2004-2005, the cyber attack field changed. At that moment, they were particularly aimed at getting profit from defending the notion of *cyber crime*. It is during this time when spam messages containing *Malware* and *Scamware* threats appear.

During 2007-2008, the cyber field changed again being mostly focused on the cyber espionage area. The first versions of *Advanced Persistent Threats – APTs* occur at this time: *Zeus* and *Stuxnet*.

After 2010, the complexity of attacks increases rapidly, just one attack including both elements of social engineering and destructive software. Specificities of attacks



Cyber threat – any circumstance or event that may represent a potential danger to cyber security

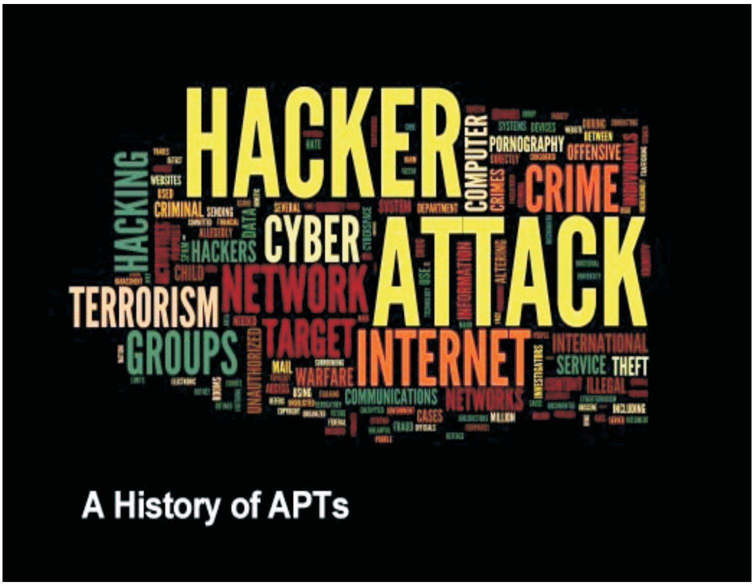
during this period are *zero-day* vulnerability exploitation, digital certificates theft and *Malware* applications polymorphism.

Persistent Cyber Threats

An *advanced persistent cyber threat* – *APT* represents a type of threats on IT systems, being most frequently associated with *Malware* activity of an IT system and vulnerability searching and exploitation of network systems, also called *hacking* activities. What is different with the *APTs* could be emphasised in two aspects: *advanced hacking* and *attack persistence*. These types of attacks are most often sponsored by an organisation or even by a nation, being connected to cyber terrorism and espionage operations. This feature allows cyber criminals to get access to more financial resources and capabilities than in case of an attack launched by a limited group of hackers. Another key aspect of *APTs* is represented by directing the attacks towards a particular system, the goal being to achieve greater impact upon the target entity than the simple abuse or confidentiality infringement.

It is well known that countries having major geopolitical interests resort to cyber espionage actions. Considering this type of threats to national security, military capabilities are developed simultaneously aiming to prevent and counter similar attacks that come from hostile nations.

The original term of *persistent threat* is related to a concept initiated by the US security agencies. Typically, the term may be used for any type of attack

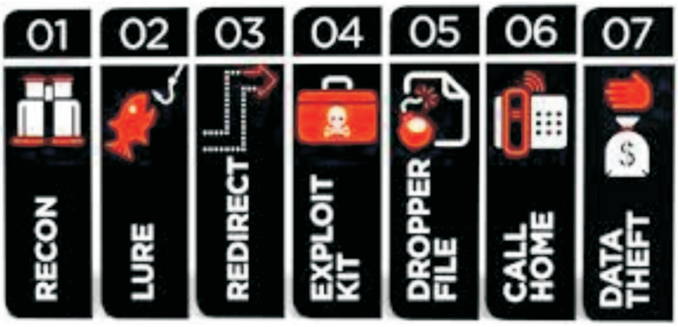


under development, active and directed towards a target for which the impact is extreme, such as the national defence system or even large organisations. Although the term *advanced* describes the use of advanced technologies, this phrase is not commonly applicable considering that an *APT* may use simple *Malware* applications, infiltrated in many systems, the way in which privileges are escalated making this threat an advanced one.

An adversary that possesses advanced expertise and significant resources, which allow it to develop attack capabilities with the purpose of reaching own goals, can use many attack vectors (IT, psychological, deceiving). These objectives are usually set in order to establish support/levers and to expand the existing ones in the technological and information infrastructures of the target organisations, with the aim of information exfiltration, undermining or obstructing the critical missions of a program or of the entire organisation. The implementation of these vectors is most commonly achieved in order to increase the success rate of future attacks.

A persistent threat pursues its goals repeatedly for a long time, adjusts to adversaries' resisting efforts and is determined to maintain its necessary level of interaction in order to carry out the proposed actions.

Previous descriptions represent a base for defining and understanding the differences between traditional attacks and *APTs*. The interaction with a command and control server, the repetitive character of the actions for the purpose of reaching the goals, the adjustment to the attacked environment and the attacks persistence create these differences. The question is *"Who is behind an APT?"* since the responsible entity cannot be established exclusively based on the sporadic activity of a *Malware* application, but it is connected to an organisation supporting strategic aims. Financial backing is most of the time achieved by a nation, the main reason being the legislative permissiveness in the IT crimes field, the international legal framework not being standardised in order to define the cyber attack actions. Firstly, the main goal of the *APTs* is to extract information from the IT systems, that being relevant for the research activities, documents considered the organisation's intellectual property, internal documents of the organisation and many more. The advanced character of the *APT* attacks is also provided by their ability to perfectly adjust to the organisation's network traffic, in order to sufficiently interact as to reach their purposes. The masking and changing abilities according to the environment represent events difficult to be detected and investigated by security experts, the efforts to stop the *ATP* attacks being often unsatisfactory.



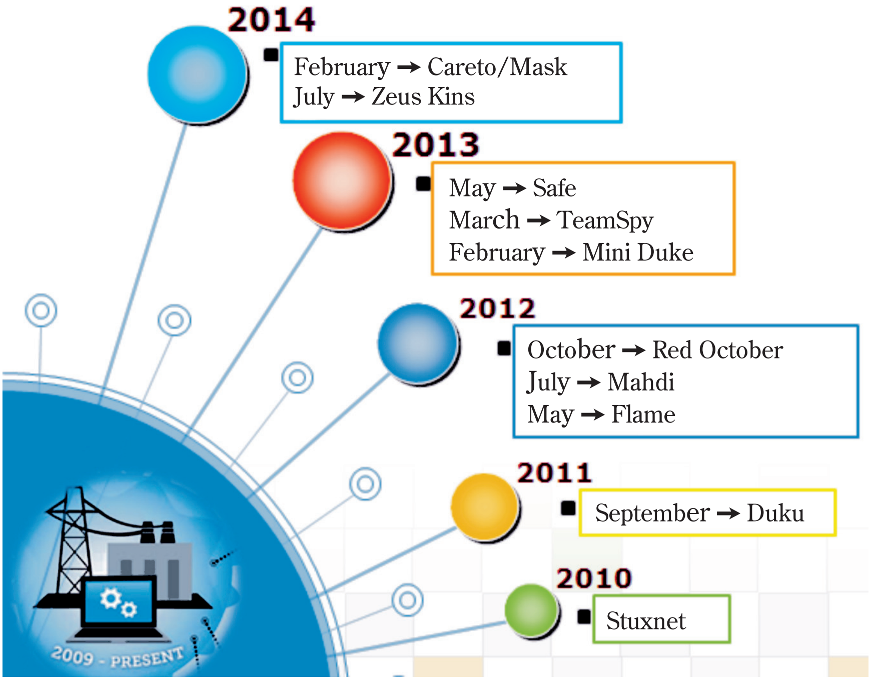
Besides their capability to adjust and remain undetected, this type of attacks is also characterised by persistence. For instance, traditional cyber threats most often attempt to exploit vulnerability. They can change their objectives towards a less safe sector if they cannot penetrate their initial targets. Particularly at this moment of the attack, *APTs* will continue their actions. *APTs* determination and repeated efforts to reach their goals are meant to create the means and methods to continue attacking after a failure.

The attackers will go on attempting to attack subsystems until vulnerabilities are identified and escalated in order to fulfil their goals. This happens because people and groups behind these attacks are motivated to reach their objective and possess the necessary means to back persistent attacks and, based on past knowledge, to launch future attacks, particularly *zero-day* attacks against organisations.

These aspects are mostly deduced from an *APT* specific signature, the fact that it is persistent and always developing. While a simple *Malware* application can be used in an initial attack, in case it faces any resistance, the attack is meant to develop, more complex software being used. The aim of an *APT* is to compromise a specific IT system and to obtain information or data, discovering the organisation's objectives, therefore defining this category of threats, making a separation from other *hacking* attempts that are carried out with the purpose of perturbing normal commercial activities, giving a boost for the attempts to sabotage a system.

APT complexity resides in the fact that such attacks use many attack vectors in order to reach their target: *spear phishing* attacks for financial data gathering, *web-based* attacks for personal information collection, and *trap files* attacks for confidential/sensitive information.

Another feature of these attacks is represented by the fact that attackers work in teams. Those interested in getting information recruit people and provide resources in order to meet their goals.



Furthermore, the *Malware* becomes more and more intelligent, being able to change itself constantly, from the way of naming the files to the way of compressing or encrypting the transfer.

The newest and most frequent cyber attacks on **governmental IT systems** have been of *APT*-type. Among them, the most famous are:

a) The *"Red October"* Campaign

In early 2013, there was a cyber alert in Romania due to a governmental CIS threat, known under the name of ***"Red October"* cyber espionage (ROCRA)** campaign. It was characterised by a gradual process based on complex, well targeted, cyber attacks, using combined methods for each stage of the attack.

In order to disseminate the *Malware* code, social engineering techniques were used, concluded with *spear-phishing* attacks against targets of strategic interest (diplomatic, governmental, military, energy etc.). A specificity of *ROCRA* operation was the way of proliferating the attacks, this case involving only a refined strategy for selecting, documenting and attacking the **pre-established targets**, and not massive infection attacks.

ROCRA campaign largely compromised IT systems all over the world, not only in Romania.

b) MiniDuke

In **February 2013**, experts from many IT security companies published the outcomes of investigations on cyber security incidents where applications exploiting the vulnerabilities of Adobe Reader (pdf files) were used, which was called *MiniDuke.*

IT examinations proved that *MiniDuke* virus acted sequentially, in three stages, directed to extract information from the governmental IT systems in **Ireland, Belgium, Romania, Portugal, the Czech Republic** and other institutions (for instance a medical services provider in the **USA** or other organisations in **Japan**, **Brazil** etc.).

MiniDuke creators use many ways of connecting to the command and control servers. In the first stage, the virus uses Google Search in order to find some information, and then it uses Twitter mail service to search for the *tweets* of certain pre-established users. If the targeted system corresponds to predefined requirements, the virus uses Twitter, without the user's permission.

Once the infected CIS is connected to the command and control server, a larger *backdoor* is uploaded, and this backdoor performs some basic operations such as **copying, moving** or **removing files**, **creating files** or **blocking some actions**, as well as downloading and **executing** a new virus. In this last phase of execution, the virus connects to two servers, one in **Panama**, and the other in **Turkey**, in order to receive instructions from the attackers.

c) *"TeamSpy"* Campaign

On 21 March 2013, a **cyber espionage campaign** was detected, called ***TeamSpy***, initiated on **05.12.2012**, which was directed towards the CIS belonging to governmental structures in many countries. The cyber attack was aimed at some **NATO and EU member states**, and the main detection mechanism for CIS disclosure was the existence of some connections with the **command and control servers**.

With the intention of infecting the CIS, some old vulnerabilities of Adobe Reader, Adobe Acrobat and Oracle Java applications were exploited.

d) *"SAFE"*

In May 2013, *Trend Micro/Canada Security Company* identified an *APT*, called *"**SAFE**"* attempting to collect data and information from the CIS connected to the Internet belonging to public, private, governmental, research institutions and others. According to the evaluation report published by the company, **12,000 IP unique addresses** were identified. The addresses belonged to the compromised CIS that connected to the command and control servers, among which **248** came from **Romania**.

The attack vector used by *"SAFE"* is based on the use of social engineering techniques aiming certain targets, by sending some e-mail messages containing destructive attachments, a vulnerability of Microsoft Office applications being exploited.

e) *"Careto/ The Mask"*

In February this year, many cyber security companies reported to have identified a cyber attack campaign called *"Careto"* or *"The Mask"*. This is one of the most advanced IT espionage operations discovered lately and is directed against institutions and companies in more than 30 countries.

The experts who evaluated this advanced threat established that the campaign was behind some cyber espionage operations starting in 2007. The specificity of *"The Mask"* is rendered by the complexity of the tools used by the attackers, including highly sophisticated *Malware*, *a rootkit*, *a bootkit*, having versions adjusted to Mac OS X and Linux operating systems, and, most likely, versions for mobile devices operating on Android and iOS (iPad/iPhone).

f) *"ZeuS-KINS"*

In July this year, a new threat was discovered in the cyber space, which, based on the IT evaluation reports published by the security companies, was identified in the IT systems belonging to many entities in Romania. Among the entities affected, there are persons, public and private organisations from various domains. This threat was called *"KINS" (Kasper Internet Non-Security)* or *"ZeuS-KINS"* because it was discovered that most of the source code of the famous *"ZeuS"* virus family was used.

Consequent to analysing the affected systems, the *Malware* specific characteristics were identified, derived from the *"ZeuS"* virus, to which new code elements were added, which were specific to other cyber attack campaigns such as *"Power Loader"*, *"Carberp"* and *"SpyEye"*. By developing these capabilities of the virus, persistence mechanisms on the infected systems were ensured.

The impact of this *Malware* infection is high, the attacker having therefore full access to the affected CIS and being able to monitor the services accessed by the users and exfiltrate confidential data, with particular interest in access credentials to e-mail accounts, banking sites, social networking sites etc.

The *"KINS" Malware* may easily affect the CIS with the Windows operating system, while for the versions that passed the support period, particularly the XP, its identification becomes more difficult. The infection vector is based on using the *spear phishing* techniques, by sending *spam/scam* personalised emails to certain users, using the target's language. The way of assessing the behaviour of the *Malware* and the attribute association are even more difficult because they are directed to command and control servers continuously modified.

The main goal of the attackers is to collect confidential information from the infected systems. Information includes official documents, various encoding keys, VPN configurations, SSH keys (meant to identify a SSH user or server) and RDP files (used by the Remote Desktop Client to automatically open a connection with the reserved computer).

The experts in cyber security succeeded in identifying five distinct stages in this threat's life cycle:

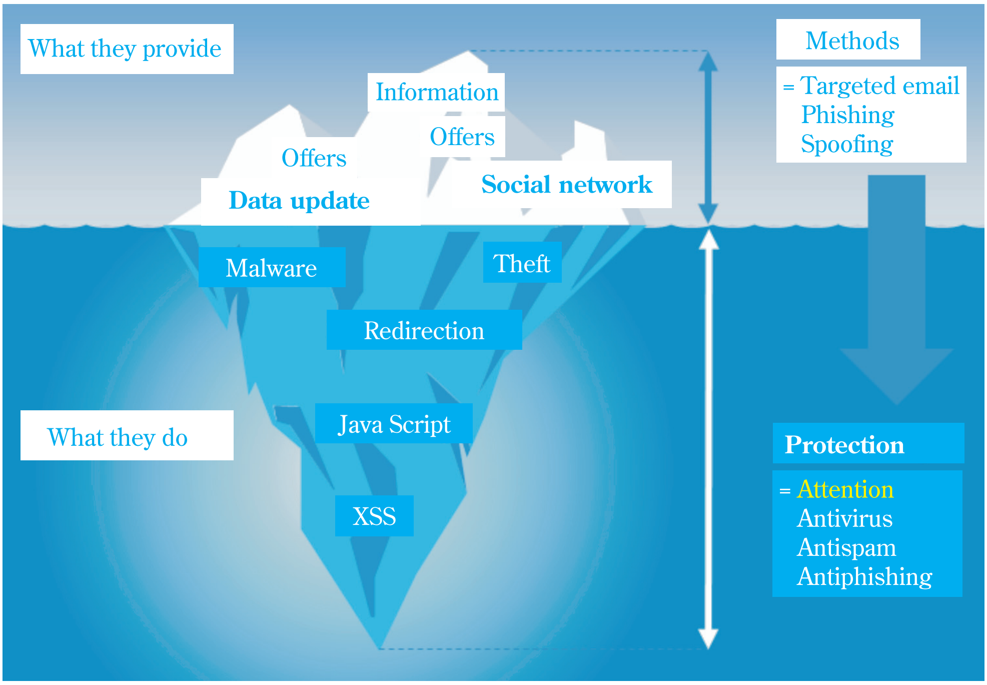
- *Stage 1*: initial intrusion through vulnerability exploitation → a group of users receives *phishing* messages. It is enough for a user to open the attachment containing the *Malware* code and the attack passes to the offensive phase;
- *Stage 2*: installing destructive software at the level of the disclosed system → CIS is remotely accessed using *backdoor* applications;
- *Stage 3*: attack expansion into the network or towards other interconnected systems → the attacker gets access rights at the user or computer level, subsequently initiating side spreading;
- *Stage 4*: achieving connections with the command and control servers → the interest data are collected and the ways through which is achieved data exfiltration are checked, by means of communicating with the command and control servers;
- *Stage 5*: targeted information and data exfiltration → the data obtained are exfiltrated using encrypted communications and files to servers which have been compromised.

Current cyber threats are able to avoid conventional security mechanisms by using certain attack techniques that pursue the identification of existing vulnerabilities and their exploitation, acquiring an access point to IT and communications systems, downloading IT viruses, using encryption means for data and information exfiltration, while the users cannot detect an abnormal behaviour.

Defence against cyber attacks is highly complex and entails much more than the use of non-technical procedures or a single security system. As a quick reaction to IT aggressions, experts have attempted to define new cyber defence solutions, materialised in a complex set of offensive and defensive actions.

Current protection solutions must be kept and must comply with the principle of defence- in-depth.

In order for an *APT* to be successful, attackers must acquire data about the target. Thus, deceit is most frequently used. According to cyber security, deceit represents a way of conducting criminal activity for the purpose of acquiring some confidential data such as access data for banking applications, e-commerce applications (i.e. eBay or PayPal) or information on credit cards using manipulation methods related to the identity data of a person or institution.



a) Targeted email is represented by messages directed exclusively to one person or a specific group of persons thoroughly evaluated in advance, potentially by means of social engineering, with the purpose of fraudulently acquiring control over a person's confidential data;

b) Phishing is the name given to attempts to fraudulently acquire control over a person's confidential data (for example, the data on a credit card, a banking account, and, in our case, the e-mail address and the password to the PayPal account).

The term reminds of the English term (identically pronounced) used for fishing – and, truthfully, because *phishing* means *“navigating on the Internet sea”* hoping that someone would grab the bait and it is part of the *social engineering* process;

c) Spoofing is an act (obviously illegal) to pretend having another identity than the real one, or masking the actual sender, with the aim of winning a person’s confidence, thus getting access to his/her personal data (also known as identity theft).

Organisations with cyber security responsibilities develop evaluation platforms in order to investigate the *APT* modus operandi so as to become able to counter this type of attacks. The main direction is to implement *“What If Scenarios”*. These scenarios allow cloning and installing the organisation’s security levels in safe environments where the access to information is simply presumable, thus deducing the vulnerabilities that may be exploited and assessing the possible consequences of a cyber attack on own infrastructure. Following the evaluation post-attack on the environment isolated and deliberately cloned for this purpose, security products can be created, installed and tested, which are able to be integrated into the organisation’s infrastructure. This way, risk tolerance can be assessed and cost constraints can be considered.

Recent studies published by key cyber security companies reveal that the greatest threat to organisations is represented by the 2% of the threats that cannot be blocked with the current security solutions. Flexible evaluation programs for cyber threats are focused on countering the 2% whereas, strategically, measures are undertaken to diminish the impact of potential attacks. Thus, an attempt has been made to implement a key measure in the IT security strategy of the organisations referring to assuming compromise on the system functioning under the circumstances of an attack or services’ disruption, when the source or the attack method cannot be identified.

Internet Resources

1. http://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/unveilingthemask_v1.0.pdf
2. http://technology.info/advanced-persistent-threat-interview/
3. http://www.fierceitsecurity.com/story/advanced-persistent-threat-not-so-much-says-researcher/2014-08-07
4. http://www.go4it.ro/internet/kaspersky-lab-a-descoperit-the-mask-una-dintre-cele-mai-avansate-operatiuni-de-spionaj-cibernetic-12062544/
5. https://www.nsslabs.com/reports/cyber-resilience-%E2%80%93-it%E2%80%99s-not-98-you-catch-matters-it%E2%80%99s-2-you-miss
6. http://www.trendmicro.com/cloud-content/us/pdfs/business/datasheets/wp_apt-survey-report.pdf
7. http://www.webcti.com/advanced-persistent-threat-management/
8. http://www.wisegeek.com/what-is-an-advanced-persistent-threat.htm.

STATES SANCTIONS POLICY

– A Form of Undeclared War –

General (r.) Dr Mihail ORZEAŢĂ

Following a primary assessment of the impact of sanctions on the international community, the author notes that they were often imposed in contradiction with the UN Charter provisions, and the global organisation could not intervene, which has diminished its importance and credibility. In particular, the author presents the effects of imposing such sanctions in the political, economic-financial, social and security fields, starting with the goals set by the initiators and ending with the decline in the living standards of the people in the sanctioned states and their growing hostility towards the initiators of sanctions, which have led to internal and international tensions and reduced regional and even global security.

***Keywords**: Cold War; air strikes; Russian Federation; regional security; trade*

1. Brief History

The use of the notion of *sanctions* to reduce or restrict the volume of economic, financial, cultural, scientific, technological, military or other exchanges between states is a way to avoid breaching the UN Charter provisions. The ban on imports or exports, irrespective of their nature, is a form of embargo. However, as embargo between states can be imposed, according to the UN Charter, only if it is authorised by the Security Council[1], the *"euphemism" sanctions* is used. Anyone who is well informed can understand that *"sanctions"* represent a form of embargo or even blockade. Nevertheless, the world organisation can respond only by the General Assembly resolutions[2], which do not have the force to impose measures, as the Security Council can do.

General (r.) Dr Mihail Orzeaţă – former Deputy Chief of the Romanian General Staff, Professor, *Apollonia* University, Iaşi, Doctoral Supervisor, *"Carol I"* National Defence University, Bucureşti.

[1] UN Charter, Chapter VIII, see http://www.un.org/en/documents/charter/chapter8.shtml, retrieved on 05.05.2015 *("But no enforcement action shall be taken under regional arrangements or by regional agencies without the authorisation of the Security Council")*.

[2] Joy Gordon, *The US Embargo against Cuba and the Diplomatic Challenges to Extraterritoriality*, *The Fletcher Forum of World Affairs*, Vol. 36:1, Winter, 2012, pp. 63-79, see http://www.fletcherforum.org/wp-content/uploads/2013/12/Gordon_36-1.pdf, retrieved on 03.05.2015 (Since 1992, the UN General Assembly has passed annual resolutions condemning the ongoing impact of the US embargo against Cuba); see also *Backing Ukraine's Territorial Integrity, UN Assembly Declares Crimea Referendum Invalid*, *UN News Centre*, 27.03.2014, http://www.un.org/apps/news/story.asp?NewsID=47443â.VT9DfdGdKM9, retrieved on 10.04.2015.

The situation is determined by the UN organisation and functioning, which allow the Security Council permanent members to veto any decision that affects their interests[3]. History teaches us that *"sanctions"* are usually initiated by the great powers that are permanent members of the Security Council, the UN General Assembly resolutions affecting only their image among the other member states. The resolutions can also influence the other states to take legal measures (in the spirit of international regulations) not to comply with the initiators request to impose *"sanctions"*/embargo[4].

The *Cold War* was a *"series of sanctions"* in the political, diplomatic, economic, financial, cultural and military fields, *"spiced"* with continuous and increasingly sophisticated and efficient propaganda, as experience was gained and the methods and means of influencing individuals and communities were developed.

The **Berlin Blockade by the USSR**, followed by building the fence and then the wall to divide the city, were among the first and best known *"sanctions"* concerning the East and the West[5].

The declared goals of the Berlin blockade – to occupy the Western part of the city by the Soviet forces and to force the US, British and French forces out – were not met because the USA, which decisively contributed to the victory in the Second World War, should have considered defeated by the rival for dominating the world – the USSR. Because its credibility as a great power in the international arena was at stake, the US airlifted[6] in supplies to provide the inhabitants of West Berlin with the goods necessary to survive and, implicitly, the moral support not to surrender to the Soviets. Neither the fence nor the Berlin Wall, built by the Eastern German authorities, could solve the problem of the inhabitants of East Berlin illegal immigration to West Berlin and, subsequently, to the Federal Republic of Germany. It is true that illegal immigration was reduced and most of those who tried to cross over the fence[7] or the wall were imprisoned or killed,

[3] *UN Security Council Action on Crimea Referendum Blocked*, *UN News Centre*, 15.03.2014, see http://www.un.org/apps/news/story.asp?NewsID=47362#.VT9CTtGdKM8, retrieved on 10.04.2015.

[4] Joachim Roy, *Cuba, the United States and the Helms-Burton Doctrine: International Reactions*, University Press of Florida, Gainesville, 2000, p. 84, apud Joy Gordon, *The US Embargo against Cuba and the Diplomatic Challenges to Extraterritoriality*, *The Fletcher Forum of World Affairs*, Vol. 36:1, Winter, 2012, p. 71, see http://www.fletcherforum.org/wp-content/uploads/2013/12/Gordon_36-1.pdf, retrieved on 03.05.2015.

[5] Editors of Encyclopaedia Britannica, *Berlin Blockade and Airlift, Europe (1948-1949)*, *Encyclopaedia Britannica*, updated 24.02.2015, see http://www.britannica.com/EBchecked/topic/62154/Berlin-blockade-and-airlift, retrieved on 04.05.2015.

[6] D.M. Giangreco and Robert E. Griffin, *The Berlin Airlift*, Harry S. Truman Library and Museum, see http://www.trumanlibrary.org/whistlestop/study_collections/berlin_airlift/large/, retrieved on 04.05.2015.

[7] *Before the Berlin Wall, People Escaped through a Wire Fence*, *pinterest.com*, see https://www.pinterest.com/pin/100486635411375676/, retrieved on 03.05.2015.

but the desire of the inhabitants of East Berlin to evade the *"communist camp"* could not be definitively stopped *(photo 1)*.

Photo 1: People in East Berlin escaping through the wire fence dividing East and West Berlin[8]

The **Cuban Missile Crisis** was an important episode in the *Cold War* employing *blockade* – another term that requires the initiator or initiators to request and obtain the Security Council approval to impose restrictions of any kind, in relations with other states.

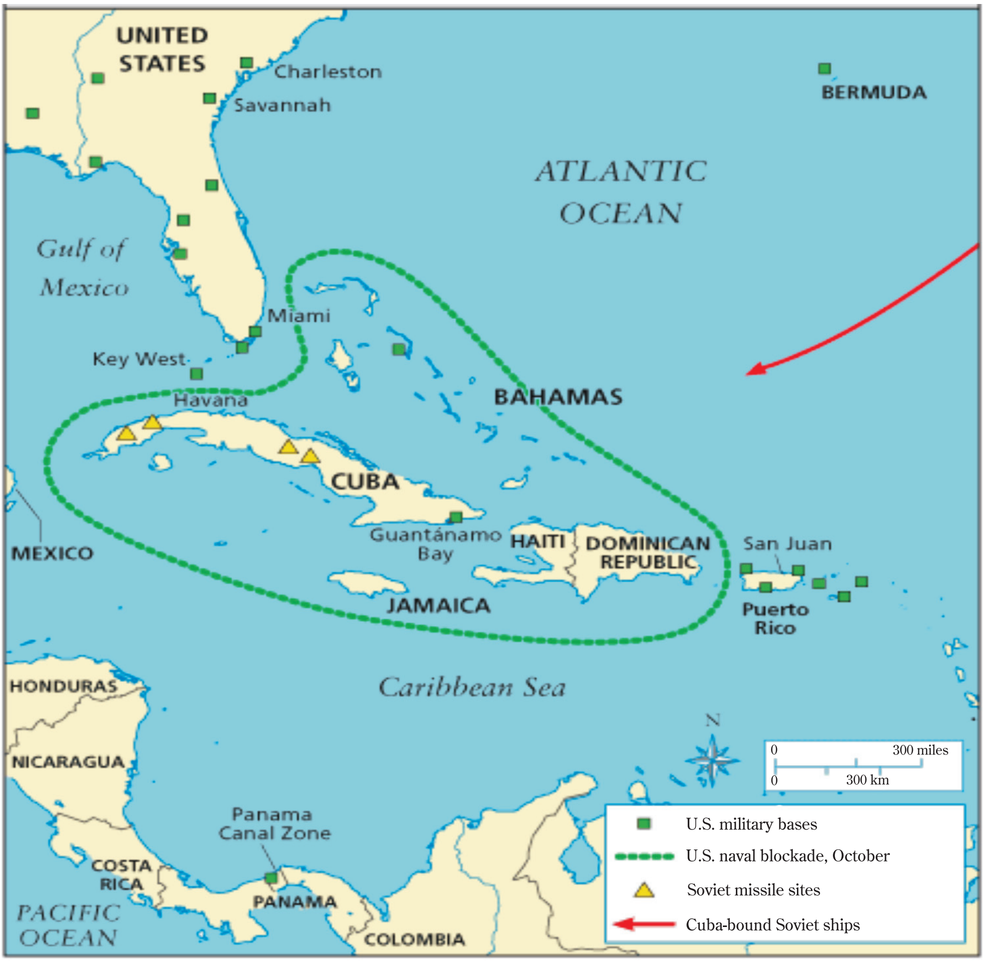
Discovering a Soviet-made medium-range missile base under construction on the territory of Cuba[9], the Kennedy Administration decided to proclaim *"quarantine"* to prevent any ship from entering or leaving Cuba, without the US Navy permission (details in *photo 2*)[10].

The use of the notion of *"quarantine"* served two purposes. The first was practical – to control the maritime connections of the regime in Havana. The second was political-strategic, namely to avoid the use of the notion of *"blockade"*, not to be accused of violating the UN Charter, as well as to warn the USSR that the USA established the *"red line"* whose breach would have meant military confrontation. *"Quarantine"* materialised President Kennedy intention to reduce

[8] *Ibidem.*

[9] *Cuban Missile Crisis,* John F. Kennedy Presidential Library and Museum, see http://www.jfklibrary.org/JFK/JFK-in-History/Cuban-Missile-Crisis.aspx, retrieved on 03.05.2015.

[10] Source: *What Cuban Missile Crisis Can Teach Us about the Nuclear World War 3*, 29.07.2014, see http://www.investwithalex.com/what-cuban-missile-crisis-can-teach-us-about-the-nuclear-world-war-3/, retrieved on 03.05.2015.



© 2003 Facts On File, Inc.

Photo 2: Cuban Missile Crisis, 1962

the psychological impact related to the adopted measure on the leaders in the Kremlin and to spare their vanity. If the USSR had breached *"quarantine"*, then it would have been accused of triggering a military confrontation, which could even evolve into a nuclear war. If Soviet ships had complied with *"quarantine"*, then the Kremlin would have conceded diplomatic defeat, which actually happened, diminishing the USSR prestige and resulting in overthrowing Nikita Khrushchev, in 1964[11].

The US punitive measures against Cuba have continued as a total embargo (economic, political, diplomatic, military and cultural sanctions[12]), which is in force

[11] Nikita Khrushchev, *History Learning Site*, 2014, see http://www.historylearningsite.co.uk/nikita_khrushchev.htm, retrieved on 03.05.2015.

[12] Gerhard Peters and John T. Woolley, *Proclamation 3447 – Embargo on All Trade with Cuba*, John F. Kennedy, President of the United Sates, 3 February 1962, *The American Presidency Project*, see http://www.presidency.ucsb.edu/ws/?pid=58824, retrieved on 04.05.2015.

even today, without contributing to the change of the country political regime or to the overthrow of the regime established by Fidel Castro[13]. The US President, Barack Obama, requested the Congress to lift the embargo, on 15 January 2015[14], but the initiative faced opposition[15], and the US legislative body has not come to a decision yet.

Political, economic, financial and military sanctions were also imposed on Iraq by the UN[16], after the regime in Baghdad decided to invade Kuwait on the night of 1 to 2 August 1990, under the guise of helping a group of revolutionaries to overthrow the emir, who was considered corrupt. The declared goal of the sanctions was to liberate the emirate from the Iraqi troops, which failed to be met, and the Security Council decided to use force to achieve the set goal. The armed intervention, known as the *First Gulf War* (January-April 1991), was carried out by a Multinational Coalition Force, led by the USA, which forced the Iraqi Armed Forces to withdraw from Kuwait[17]. The sanctions on Iraq continued after the end of the First Gulf War[18], to determine Saddam Hussein to renounce developing the programmes to obtain weapons of mass destruction, especially nuclear ones. Even after 12 years of sanctions the goal was not met[19] and then military force was again employed against Iraq, without the UN approval, by a *"Coalition of the Willing"*[20], also led by the USA, action that was known as the *Second Gulf War* (2003).

Political, economic, financial and military sanctions were also employed in an attempt to solve the successive crises in former Yugoslavia between 1991

[13] Daniel Griswold, *Four Decades of Failure: The US Embargo against Cuba*, Cato Institute, 12.10.2005, see http://www.cato.org/publications/speeches/four-decades-failure-us-embargo-against-cuba, retrieved on 04.05.2015.

[14] *President Asks Congress to Lift Embargo against Cuba*, *ABC NEWS*, 20.01.2015, see http://abcnews.go.com/Politics/president-congress-lift-embargo-cuba-sources/story?id=28358404, retrieved on 03.05.2015.

[15] News Released by Staff, *Governor Scott: Lifting Cuban Embargo Could Hurt Florida Agriculture*, Florida Governor, 22.04.2015, see http://www.flgov.com/2015/04/22/governor-scott-lifting-cuban-embargo-could-hurt-florida-agriculture/, retrieved on 03.05.2015.

[16] *UN Arms Embargo on Iraq*, Stockholm International Peace Research Institute, Stockholm, last updated 24 October 2012, see http://www.sipri.org/databases/embargoes/un_arms_embargoes/iraq, retrieved on 03.05.2015.

[17] Thomas E. Ricks, *Fiasco. The American Adventure in Iraq*, Penguin Books London, UK, 2007, p. 3.

[18] *UN Security Council Resolution 687 (1991)*, Stockholm International Peace Research Institute, Stockholm, last updated 24 October 2012, see http://www.sipri.org/databases/embargoes/un_arms_embargoes/iraq/un-security-council-resolution-687-1991, retrieved on 03.05.2015.

[19] Eric Laurent, *Războiul familiei Bush*, Editura Vivaldi, București, 2004, pp. 223-225 (Although under the embargo of the United Nations, which had to be respected by all member states, Iraq sold oil through Jordan, and obtained the necessary funds to purchase military equipment, armament and ammunition to train its army and increase its combat capability from Russia, China, Germany and other states.)

[20] Steve Schifferes, *US Names 'Coalition of the Willing'*, *BBC News Online Washington*, 18.03.2003, see https://www.google.ro/?gws_rd=cr,ssl&ei=LftKVdTtO8OvygPZgYGwCA, retrieved on 03.05.2015.

and 1999. The goals were not met and then it was decided the military intervention in Bosnia-Herzegovina (1992-1995)[21] and Kosovo (1999)[22].

Syria, Libya, North Korea and Iran were included in the so-called *"axis of evil"* because they sponsored terrorism and developed programmes for producing weapons of mass destruction. They were subject to political, economic, financial and military sanctions to make them comply with international regulations. The goals were achieved only in the case of Libya, which renounced obtaining weapons of mass destruction, for fear it should be the next target of the *"Coalition of the Willing"*, after its military intervention in Iraq in 2003[23].

Syria has been subject to sanctions since 1979[24] to present[25] and it has been the target of several Israeli air strikes on the locations suspected to be infrastructure elements of the weapons of mass destruction programmes[26].

Iran has also been the target of sanctions from Western states, following the 1980 hostage crisis and the USA and Israel allegations that they can develop programmes to produce nuclear weapons and carrier missiles. Since 2006, it has been subject to a partial embargo on the import of military nuclear technology, to which are added the embargo on Iranian armament export, in 2007, and the embargo on major conventional weapons, in 2010[27]. However, it has not renounced its nuclear programme. The Islamic Republic has not been directly militarily attacked, but the leaders in Teheran have repeatedly accused the USA and Israel of cooperating to sabotage its nuclear programme, to kill some of the most prominent experts

[21] *The War in Bosnia, 1992-1995*, *Office of the Historian*, last updated 31 October 2013, see https://history.state.gov/milestones/1993-2000/bosnia, retrieved on 03.05.2015.

[22] Robert Bideleux, *Kosovo's Conflict*, *History Today*, vol. 48, no. 11, November 1998, see http://www.historytoday.com/robert-bideleux/kosovos-conflict, retrieved on 01.05.2015.

[23] *UN Arms Embargo on Libya*, Stockholm International Peace Research Institute, Stockholm, last updated 25 October 2012, see http://www.sipri.org/databases/embargoes/un_arms_embargoes/libya/libya-1992, retrieved on 03.05.2015.

[24] Holly Fletcher, *State Sponsor: Syria*, *Council of Foreign Relations*, 01.02.2008, see http://www.cfr.org/syria/state-sponsor-syria/p9368, retrieved on 01.05.2015.

[25] *EU Arms Embargo on Syria*, Stockholm International Peace Research Institute, Stockholm, last updated 13 November 2013, see http://www.sipri.org/databases/embargoes/eu_arms_embargoes/syria_LAS/eu-embargo-on-Syria, retrieved on 01.05.2015.

[26] David Makovsky, *The Silent Strike*, *The New Yorker*, see http://www.newyorker.com/magazine/2012/09/17/the-silent-strike, retrieved on 01.05.2015 (Israeli Air Force – 4 F-16 and 4 F-15 – destroyed the Syrian nuclear installation in Al Kibar, on 5 September 2007, during an action that was similar to that in June 1981, when the Iraqi nuclear installation in Osirak was destroyed.); see also John Kettler, *Nuclear Strikes! Syria Nuked Fourth Time by Israel!*, John Kettler Investigates, see http://www.johnkettler.com/nuclear-strikes-syria-nuked-fourth-time/, retrieved on 01.05.2015.

[27] *UN Arms Embargo on Iran*, Stockholm International Peace Research Institute, Stockholm, last updated 11 October 2012, see http://www.sipri.org/databases/embargoes/un_arms_embargoes/iran, retrieved on 03.05.2015.

in the field of nuclear energy[28] and to implant destructive software in the computer networks belonging to the armed forces or other Iranian institutions[29]. The Islamic Republic has also accused Azerbaijan of offering its territory and some military bases in the south of the country to Israel to execute air strikes on the infrastructure related to Iranian programmes meant to develop weapons of mass destruction.

The history of sanctions is repeated in the Ukraine crisis, after the Crimean Peninsula secession and its integration into the Russian Federation[30], followed by the self-proclaimed independence of Donetsk and Luhansk provinces. Aiming to support Ukraine to restore its territorial integrity, the West (the USA, the EU, Canada and Australia) required Russia to return the Crimean Peninsula to Ukraine and not to support the separatist movements in Donetsk and Luhansk. Russia denied its military involvement in supporting the separatists in Eastern Ukraine and refused to return Crimea. Under those circumstances, the West has imposed political, economic, financial and military sanctions on Russia, in several *"waves"*[31].

Russia has responded to Western sanctions taking similar measures, seeming to draw inspiration from the history of the *Cold War* or the *"Lex Talionis" ("an eye for an eye and a tooth for a tooth")*. The process of mutual administration of sanctions between Moscow and the West is under development and it could escalate, but it is difficult to predict the outcome.

2. Effects of Sanctions

2.1. General aspects regarding states sanctions

Politically, sanctions have facilitated the **loss of unity**. Internally, citizens that have become unemployed and company owners that have lost money ask governments to stop sanctions and provide financial compensation. Internationally, *"sanctioned"* states seek solutions to accordingly respond to the initiators of sanctions,

[28] Julian Borger, Saeed Kamali Dehghan, *Attack on Iranian Nuclear Scientists Prompts Hit Squad Claims*, in *The Guardian*, 29 November 2010, see http://www.theguardian.com/world/2010/nov/29/iranian-nuclear-scientists-attack-claims, retrieved on 01.05.2015.

[29] David E. Sanger, *Obama Order Sped up Wave of Cyberattacks against Iran*, in *The New York Times*, 01.06.2012, see http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0, retrieved on 01.05.2015.

[30] *Backing Ukraine's Territorial Integrity, UN Assembly Declares Crimea Referendum Invalid, UN News Centre*, 27.03.2014, see http://www.un.org/apps/news/story.asp?NewsID=47443#.VT9DfdGdKM9, retrieved on 10.04.2015.

[31] Tatia Dolidze, *EU Sanctions Policy towards Russia: The Sanctioner-Sanctionee's Game of Throne, CEPS Working Document*, Centre for European Policy, no. 402, January, 2015, see http://www.ceps.be/system/files/WD%20402%20TD%20Sanctions.pdf, retrieved on 10.04.2015; see also Jeroen Jansen and Valerijus Ostrovskis, *EU Sanctions against Russia: New Targets and State of Play, DLA PIPER*, 11.02.2015, see https://www.dlapiper.com/en/us/insights/publications/2015/02/eu-sanctions-against-russia/, retrieved on 03.05.2015.

and the populations of those states get increasingly hostile to the initiators of sanctions, as they are *"punished"* to face the consequences of punitive measures. It is the case of the Muslim states in the Middle East and North Africa[32], as well as of the Serbs. This effect is actually the opposite of that expected by the initiators of sanctions, who intend to influence the population of the sanctioned states to revolt against their leaders, favouring the ascension of leaders who meet the requirements. In North Africa, the overthrow of the authoritarian regimes in Libya, Egypt and Tunisia facilitated the ascension of Islamist-extremist parties in the governing structures of the particular states[33].

Economically and financially, sanctions have resulted in the loss of some markets and the partial or integral loss of the money invested in producing the goods destined to the states subject to sanctions. Surplus products have been sold below market price or stocked, requiring additional costs. To reduce losses and to sell products, some company owners affected by economic sanctions have resorted to smuggling and black or grey markets[34]. Overall, it can be said that sanctions have favoured the development of international organised crime in the economic and financial field.

Socially, the trade tumble has resulted in the diminution up to cessation of the goods and services production in the areas affected by sanctions, which has reflected in grown unemployment rate and reduced living standard for hundreds of thousands of people.

As far as security is concerned, sanctions have spurred the arms race and spending significant sums of money to enhance the armed forces combat capability, resulting in the postponement or even cancellation of some social programmes, growing distrust and hostility among states, decreasing regional or even global security.

[32] Murtaza Hussain, *The Roots of Global Anti-Americanism, Aljazeera*, 11.12.2012, see http://www.aljazeera.com/indepth/opinion/2012/12/201212108205749534.html, retrieved on 03.03.2015.

[33] *Arab Spring. Has It Failed?*, in *The Economist*, 13.07.2013, see http://www.economist.com/news/leaders/21581734-despite-chaos-blood-and-democratic-setbacks-long-process-do-not-give-up, retrieved on 06.05.2015.

[34] Tatia Dolidze, *EU Sanctions Policy towards Russia: The Sanctioner-Sanctionee's Game of Throne*, *CEPS Working Document*, *op. cit.* (Belarus has doubled its seafood imports from Norway, Lithuania and Poland, and sold them to Russia, labelled *"made in Belarus, although it is not a littoral state"*. Belarus also imports meat from the Netherlands, Germany and Poland, to sell it to Russia, labelled *"made in Brazil"*).

2.2. Specific aspects regarding reciprocal sanctions between Western, EU and NATO states, on the one hand, and the Russian Federation, on the other hand

The estimates of the sanctions effects on Russia, the EU member states, the USA, Canada and Australia, made by some economic analysts and experts in the field, are quite contradictory. Given the relatively short period of time that has passed since sanctions were imposed, their impact is difficult to estimate, especially taking into account that some measures will have cumulative effects in the long run. For example, the interruption of the trade relations between the EU and Russia and the USA and Russia, in many fields, will require the investment and production reorientation towards other markets, generating additional costs and changes in the production process to meet the new consumers requirements.

2.2.1. The effects of sanctions on the Russian Federation

Russian Finance Minister, Anton Siluanov, appreciated, in a report presented to the State Duma, on 28.01.2015, that his country could record about 40 billion dollars losses because of direct sanctions, and about 200 billion dollars losses because the decrease in the oil and natural gas prices. In the same vein, Vladislav Inozemtsev, Director, Centre for Post-Industrial Studies in Moscow, and Visiting Fellow, Centre for International Strategic Studies in Washington, considers that Russia's direct losses will amount to about 100 billion dollars, to which other 200 billion dollars connected to foreign capital withdrawal should be added[35].

The European Commission estimates that the sanctions on Russia will result in reducing the economic growth by 1.1% in 2015, depreciation of the ruble in international markets, and the withdrawal of about 130 billion dollars foreign capital[36].

In an analysis published on 3 April 2015, *STRATFOR*, an independent global intelligence agency, mentions that, in Russia, 154,800 jobs were cut in 2014 and 127,000 in the first months of 2015, the ruble depreciates, inflation skyrockets, and there are problems with subsidisation in some regions, generating minor protests, which can amplify in the future unless the economic situation enhances and salaries are paid in due time. The idea of secession, in some areas of the Federation, has become topical again, because of the economic and social problems[37].

[35] Vladislav Inozemtsev, *Yes, Sanctions Work*, *The American Interest*, 02.02.2015, see http://www.the-american-interest.com/byline/vladislav-inozemtsev/, retrieved on 01.05.2015.

[36] Jeroen Jansen and Valerijus Ostrovskis, *EU Sanctions against Russia: New Targets and State of Play*, *DLA PIPER*, *op. cit.*

[37] *Amid an Economic Crisis, Russia Contains Dissent, Analysis*, *STRATFOR*, 03.04.2015, see https://www.stratfor.com/analysis/amid-economic-crisis-russia-contains-dissent, retrieved on 10.04.2015.

Moreover, opinion polls indicate the perception of an important part of the population that sanctions are meant to humiliate the Federation[38] and they are directed mainly against ordinary people and not against oligarchs. Anti-Western and especially anti-American feelings have increased significantly, as well as the confidence in President Vladimir Putin[39].

The sanctions against Russia have resulted in the reorientation of its trade to states in Asia[40] and Latin America and the initiation of measures to dethrone the dollar from the position of universal exchange currency[41].

Following the North Atlantic Council decision to stop the military cooperation between NATO and Russia, President Putin signed a new military doctrine of his country, the Alliance being considered the biggest security risk for the Federation[42] and decided to increase military spending and to intensify the armed forces real exercises[43]. To the Western states frequent requests to return Crimea to Ukraine, President Putin replies that he will employ all the measures to defend the peninsula, even nuclear weapons if necessary[44].

2.2.2. The effects of sanctions on the European Union

Assessing the impact of sanctions on the EU, Sergei Glaziev, the economic advisor to Russian President, appreciated, in November 2014, that the European Union member states could lose about 1.2 trillion dollars[45].

[38] Matthew Dal Santo, *The Shortsightedness of NATO's War with Serbia over Kosovo Haunts Ukraine*, *The National Interest*, 2 September 2014, see http://nationalinterest.org/blog/the-buzz/the-shortsightedness-natos-war-serbia-over-kosovo-haunts-11180, retrieved on 03.05.2015.

[39] Elizabeth Pond, *Russia vs. the West: The Consequences of Putin's Invasion of Ukraine*, *New Statesman*, 05.03.2015, see http://www.newstatesman.com/politics/2015/03/russia-vs-west-consequences-putin-s-invasion-ukraine, retrieved on 10.04.2015.

[40] Timothy Heritage and Vladimir Soldatkin, *Putin Looks to Asia as West Threatens to Isolate Russia*, *Reuters*, 21.03.2014, see http://www.reuters.com/article/2014/03/21/us-ukraine-crisis-russia-insight-idUSBREA2K07S20140321/, retrieved on 04.01.2015.

[41] Asad Ismi and Peter Koenig, *De-Dollarization: Is BRICS a Viable Alternative to the US Dominated World Economic System?*, *Canadian Centre for Policy Alternatives Monitor*, 22.11.2014, see http://www.globalresearch.ca/is-brics-a-viable-alternative-to-the-u-s-dominated-world-economic-system/5415375, retrieved on 22.03.2015; see also Tyler Durden, *Vladimir Putin Proposes "Eurasian" Currency Union*, Zero Hedge, 21.03.2015, see http://www.talkmarkets.com/content/global-markets/vladimir-putin-proposes-eurasian-currency-union?post=61304&utm_source=outbrain&utm_medium=referral, retrieved on 22.03.2015.

[42] Joshua Noonan, *On Russia's New Military Doctrine*, *Silkroad Reporters*, 17.01.2015, see http://www.silkroadreporters.com/2015/01/17/on-russia-new-military-doctrine/, retrieved on 03.03.2015.

[43] James T. Quinlivan, *Yes, Russia's Military Is Getting more Aggressive*, Rand Corporation, see http://www.rand.org/blog/2014/12/yes-russias-military-is-getting-more-aggressive.html, retrieved on 03.03.2015.

[44] John Hall, *Putin Threatens Nuclear War: Russian Leader Will Take any Necessary Step to Drive NATO out of Baltics and Defend Crimea*, *Mail Online*, 02.04.2015, retrieved on 05.04.2015.

[45] Valery Sharifulin, *EU May Lose 1 Trillion Euros over Sanctions against Russia – Kremlin Advisor*, ITAR-TASS, 13.11.2015, see http://tass.ru/en/economy/759450, retrieved on 01.05.2015.

The European Commission report on the impact of sanctions imposed on Russia estimates that the boomerang effect of the punitive measures, combined with similar measures imposed by Russia on the EU states, will result in a decline in the economic growth of the European Union by 0.2-0.3% and a decrease in the trade with the Russian Federation by 60%[46].

Performing a similar analysis related to the EU losses because of the sanctions imposed on Russia, Vladimir Inozemtsev considers that they will not exceed 20-25 billion Euros per year[47], amount considered insignificant compared to the EU Gross Domestic Product of 13,000 billion Euros. Inozemtsev estimates seem to be more optimistic than those of German analysts. They consider that 25% of the companies can be affected only in Germany, and at least 25,000 jobs can be cut[48].

Tatia Dolidze thinks that the worst effect of the sanctions is the *"lack of unity"*, as the states where the *"boomerang effect"* is felt most acutely request the Council of Europe to renounce sanctions and conclude direct transactions with Russia. The *"entrepreneurs"* in several European Union member states have chosen to export their products to the Russian Federation through Belarus, Kazakhstan, Montenegro and other countries that are not subject to sanctions[49].

3. Conclusions

Politically, sanctions have proved inefficient in most cases, considering the initiators declared goals, as they have not been met or they have been met only partially.

If we assess the impact of sanctions on the international community, we find out that, more often than not, they have been imposed in contradiction to the UN

[46] Jeroen Jansen and Valerijus Ostrovskis, *EU Sanctions against Russia: New Targets and State of Play*, *DLA PIPER*, 11.02.2015, *op. cit.*

[47] Vladislav Inozemtsev, *Yes, Sanctions Work*, *The American Interest*, *op. cit.*

[48] Matthias Schepp and Cornelia Schmergal, *The Boomerang Effect: Sanctions on Russia Hit German Economy Hard*, *Spiegel Online*, 21.07.2014, see http://www.spiegel.de/international/business/german-economy-hit-by-us-eu-sanctions-on-russia-a-982075.html, retrieved on 10.04.2015.

[49] Tatia Dolidze, *EU Sanctions Policy towards Russia: The Sanctioner-Sanctionee's Game of Throne*, *CEPS Working Document*, Centre for European Policy, no. 402, pp. 8-9, January, 2015, see http://www.ceps.be/system/files/WD%20402%20TD%20Sanctions.pdf, retrieved on 10.04.2015 (Hungarian Prime Minister Orban believes that the EU is *"shooting itself in the foot"* imposing sanctions on Russia and, accordingly, Hungary does not plan on *"going along"*. In 2014, Hungary and Russia signed a deal to build a nuclear reactor plus a 10 billion Euros loan. Slovakian President Robert Fico proclaims the EU sanctions to be *"meaningless and counterproductive"*, and signed, in October 2014, a 15-year Russian oil-supply deal. Poland decides to adopt a *"pragmatic policy"* towards Russia. The Czech Prime Minister uses the metaphor *"Iron Curtain"* to express the disagreement with the Russia-EU sanctions. Similarly, Finnish Prime Minister Alexander Stubb appreciates that it is not *"the right time"* for the sanctions to continue.).

Charter provisions, the world organisation having no possibility to intervene, which has diminished its importance and credibility.

Economically and financially, sanctions have resulted in losses for both sanctioners and *"sanctionees"*, a situation considered as a *"lose-lose game"* by an EU official.

Socially, sanctions have generated unemployment, a lower living standard in the countries affected by sanctions, and growing hostility to the initiators of sanctions, which have led to internal and international tensions and reduced regional and even global security.

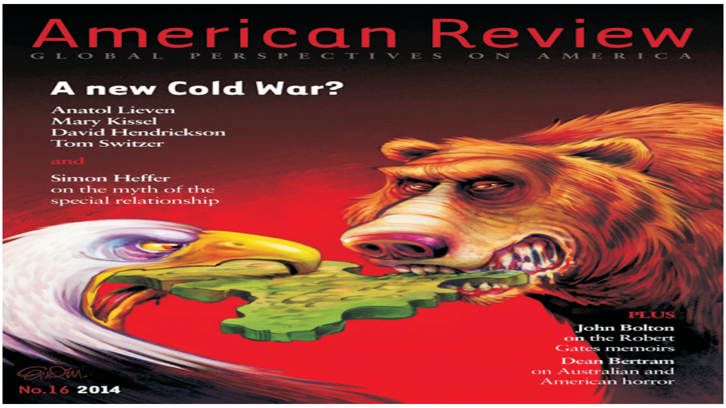


Photo 3: USA and Russia fighting for Crimea[50]

As far as security is concerned, sanctions could result in a new *Cold War*[51], and Crimea *"effect"* could *"contaminate"* other regions in Russia that have already claimed secession. Moreover, it could be the precedent other ethnic communities that are part of multinational states invoke, with consequences that are difficult to estimate.

English version by
Diana Cristiana LUPU

[50] Source: *A New Cold War?*, *American Review* cover, no. 16, 02.05.2014, see http://blog.antonemdin.com/2014/05/a-new-cold-war/, retrieved on 01.05.2014.

[51] Simon Tisdall, *The New Cold War: Are We Going back to Bad Old Days?*, in *The Guardian*, 19.11.2014, see http://www.theguardian.com/world/2014/nov/19/new-cold-war-back-to-bad-old-days-russia-west-putin-ukraine, retrieved on 30.12.2014; see also Rakesh Krishnan Simha, *Why Putin Is Winning the New Cold War*, in *Global Research*, 30.11.2014, see http://www.globalresearch.ca/why-putin-is-winning-the-new-cold-war/5417041, retrieved on 30.12.2014.

THE ROMANIAN MOUNTAIN TROOPS

– Between Historical Necessity and Present Milestones –

Lieutenant Colonel Nicolae USZKAI

During the First World War the Mountain Corps was established. It was a powerful unit, consisting of three mountain troops battalions, each of them having three mountain troops companies. They acted as a true independent unit against the German and Austro-Hungarian troops, for the first time in the campaign of 1917. Later, the author points out, during the campaign of 1918, the Mountain Corps was known as the Mountain Troops Battalion, consisting of 4,000 troops, which was considered an elite specialised force at the time.

***Keywords**: Austro-Hungarian troops; Ribbentrop-Molotov Pact; cavalry; Transylvania*

As it is known from a military perspective, mountain combat actions refer to those actions conducted in the mountains or similarly rough terrain. This type of warfare is also called *Alpine warfare*, after the Alps Mountains. Mountain warfare is one of the most dangerous types of combat actions as military structures have to survive while combating not only the enemy but also the extreme weather and dangerous or difficult terrain. The military men belonging to Mountain Troops are specialists trained and equipped to operate in mountainous environment. Dedicated mountain troops represent a relatively new phenomenon.

The history of this part of the world has highlighted the necessity of conducting actions in high mountainous areas. Therefore, in Europe, there have been units of this type, traditionally linked with the mountains. In this context, Germany's *Gebirgsjäger*, Italy's *Alpini*, and France's *Chasseurs Alpins* have been, since their establishment, highly distinctive and individual in nature. Similarly, the Romanian Mountain Troops *(Mountain Hunters)*, *Vânătorii de Munte* in Romanian, were established within the Romanian Land Forces as an operational necessity starting with the First World War.

Lieutenant Colonel Nicolae Uszkai – 2nd Mountain Troops Brigade *"Sarmizegetusa"*, Braşov.

The birth of the Romanian Mountain Troops was unexplainably late compared to other European military powers, especially considering that a great part of the Romanian borders at that time was represented by the Carpathian Mountains. A possible explanation can be the existence of the secret Treaty concluded in 1883 between King Carol I of Romania and the Triple Alliance (Germany, Austria-Hungary and Italy). Considering the treaty, Romania did not expect any aggression over the Carpathians. However, in 1883, the Romanian Mountain Artillery was established, having one battery assigned to each of the four existing Army Corps. Later, in 1892, the Mountain Artillery was re-assigned to the other Artillery Regiments. It was in 1913 when the first Mountain Gun Battalion (four 75 mm calibre batteries) was established. In 1915, the second one was established (four 63 mm calibre batteries). In 1916, the two battalions became part of the 1st Mountain Artillery Regiment having the garrison in Târgu Jiu. As the Fortress Artillery in Bucureşti was disbanded, the 63 mm calibre cannons were distributed to eight more Mountain batteries, thus resulting 16 Mountain batteries when Romania entered the First World War, in August 1916.

Paradoxically, the Romanian Armed Forces had 16 Mountain batteries but no Mountain troops and, as a consequence, the Mountain batteries were attached to battalions, divisions or tactical detachments to support them during the campaign in the autumn of 1916. However, the Mountain Troops had not been established yet even though they were obviously necessary. It would have been better if the military decision-makers at that time had taken more advantages of those two years of neutrality, analysing the lessons from the battles of other European armies and seizing the opportunity and the need to have Mountain Troops at the border with the future enemy.

As far as other European armed forces were concerned, specialised mountain troops were established in the Italian Army in 1873, their example being followed by other armies. In the First World War, there were Alpine Troops in the French Armed Forces. There were also such troops in the German and Austrian Armed Forces. They later fought against the Romanian troops in Sibiu and Dragoslavele. There were some initiatives with regard to establishing mountain troops in Romania too, discussed in some military publications of the time. We wonder why the Romanians did not follow the example of the Italians, as partners in the Triple Alliance, earlier. An answer may be the fact that they gained experience in this respect fighting for their independence against the Austrians in 1861. Another explanation may be that King Carol I did not want the establishment of specialised mountain troops to be perceived as being a provocative act against an ally. However, King Carol I died in October 1914, three month after the beginning of the First World War, and the Romanian Armed Forces could capitalise on the lessons learned from other European fronts in many ways including, also, the establishment of specialised troops, especially as King Ferdinand and his wife, Queen Mary, were interested in the Entente Powers. We also wonder what the end-state of the 1916 autumn campaign would have been if there had been specially trained mountain troops since 1914. It is less likely to have been different, considering all the factors involved in the Eastern Front, the lack of support from other fronts and the forces ratio. However, the result of many battles inside the Carpathians could have been different. Let us mention here the second battle on the Jiu River, when the major breach on 1/14 November was made in a very narrow gorge in the mountains used by the German troops. Here, definitely, the Mountain Troops could decisively influence the operations. Taking into consideration their achievements in the summer campaign of 1917, just few months after their establishment, it can be concluded that if we had had such specialised troops since 1914, the operations in the Carpathians in the autumn campaign of 1916 could have had other results. Furthermore, the Romanian forces fought against both German and Austrian-Hungarian Alpine Troops; maybe it was the major factor that led to the establishment of the Romanian Mountain Troops.

The Romanian Mountain Troops were thus established on 3 November 1916, during the First World War, representing, from the very beginning, an elite speciality in the Romanian infantry. Mountain Hunters have been a well trained force and, since 1916, fighters belonging to mountain troops have demonstrated their ability to defend the territory of the country. It was mainly demonstrated during the First and the Second World Wars. By their courage, proficiency and self-sacrifice they demonstrate that they are able to provide security for the Romanian people by accomplishing the missions they are assigned.

During the First World War, the Mountain Corps was established as a strong unit consisted of three mountain battalions, each of them having three mountain companies (total strength up to 1,980 troops). They acted, as a strong independent unit, against the German and Austrian-Hungarian armies in 1917 campaign. During 1918 campaign, the Mountain Corps was known as the Mountain Troops Battalion. Even though it was called battalion its strength was up to 4,000 troops. In 1919, during the campaigns in Transylvania and Hungary, this unit was known as the Mountain Troops Regiment. In the interwar period, the Romanian Mountain Troops had, initially, two divisions with several brigades, focusing their training on mountain warfare.

On 1 July 1923, the new Mountain Corps was established, at same time with the 1st and 2nd Mountain Divisions, large units designated to conduct combat actions in the high mountainous areas in the Carpathian Mountains. At the beginning of the Second World War, the Mountain Corps consisted of four Brigades (1st-4th) made up of twelve Mountain Groups (1st-12th), each having two battalions. There were 24 Battalions (1st-24th) out of which 16 were active, operational units, very well trained and equipped, and 8 (17th-24th) were formed after the general mobilisation, being thus less trained to conduct actions in the mountains. In that context, a Mountain Brigade had the following main structure: six Battalions, one Mountain Artillery Group (1 or 2 Battalions of 75 mm or 76 mm Mountain guns and one Battalion of 100 mm Mountain howitzers) and one Mountain Pioneer Battalion. A Mountain Battalion had three companies, each company having three platoons, and each platoon three groups. It also had a heavy weapons company made up of three machine-gun platoons (4 Schwarzlose/ZB-53 each) and one mortar platoon (4x Brandt 81.4 mm). The Rifle Platoon was equipped with one 60 mm Stokes Brandt Mortar and 3xZB light machine-guns, one for each group.

Like the Romanian Cavalry, the Mountain Troops were better trained than regular infantry. Initiative was more developed at battalion level. Battalions were properly trained and equipped to fight in mountain areas, but the fact that they did not have enough artillery made them vulnerable in open terrain. The Mountain Corps also had a mounted battalion, a *"mountain train"* and a hospital company as combat service support units.

At the beginning of the Second World War, the Mountain Corps was made up of the 1st, 2nd and 4th Mountain Brigades. The 3rd Mountain Brigade was stationed on the border with Hungary. On 3 July 1941, the Mountain Corps started its military actions in the Second World War in order to liberate Bucovina and Bessarabia, Romanian territories taken by the Soviet Union in accordance with the Ribbentrop-Molotov Pact of 1940. After the forced crossing of the Prut River, alongside the German troops, the Mountain Brigades conducted heavy and bloody combat actions on the nowadays territory of Moldova, reaching even the northern shore of the Sea of Azov. At the end of the 1941 campaign, the 2nd Mountain Brigade was redeployed to Romania and the 1st and 4th Mountain Brigades remained to conduct combat actions in Crimea. On 15 March 1942, the Mountain and Cavalry Brigades became Divisions. This measure was taken in order to emphasise the Romanian contribution to the war effort against the USSR. In July 1942, the 2nd and 3rd Mountain Divisions were sent on the new front lines and took part in the campaigns in the Caucasus and in Kuban area, reaching the south of the Caucasus Mountains, at Elbrus, Grozny and Vladicaucasus.

Considered elite troops, the Romanian Mountain troops took part in the Second World War on the Eastern Front in some of the most difficult battles, including the battles of Sevastopol and Stalingrad, where their performance lived up to their reputation. In fact, all their commanders from brigade level and up were awarded the *Mihai Viteazul* Order (the Romanian highest combat order) and the *Knight's Cross of the Iron Cross* (the German highest combat order). After other difficult actions on the Eastern Front, during 1943 and 1944 campaigns, in August 1944, Romania broke the military alliance with Germany and joined the United Nations with all its forces, starting the war against the German and Hungarian armed forces, in order to liberate the Northern Transylvania, lost following the Vienna *Award* in 1940.

On 30 August 1944, the Mountain Divisions began the battle against the German and Hungarian troops, liberating the Romanian territory, and continued to fight on the territory of Hungary and, after that, on the territory of Czechoslovakia, in the Javorina and Tatra Mountains. The Mountain Divisions ended the Second World War near Prague, on 12 May 1945.

The death toll among the soldiers from Mountain Troops was heavy during the Second World War. After their redeployment on the national territory, the Mountain Divisions resumed their peace establishment in the garrisons they belonged to. Soon, there was a turn in their history. As they were very proficient in the fights against the Soviets, being called *"green devils"* by them, the Soviets pushed the new communist leadership of the Romanian People's Republic to disband the Romanian Mountain troops, step by step. Thus, on 14 April 1961, the 2nd Mountain Brigade, the last of the largest units of the kind in the Romanian Armed Forces, was disbanded, fact that ended the first part of the Romanian Mountain Troops history. About three years after that abusive dissolution, the Great National Assembly, the legislative body of Romania at that time, decided, on 14 October 1964, to re-establish the Mountain Troops starting with the 2nd Mountain Brigade, which today is one of the representative units of the Romanian Land Forces. Between 1964 and 1990, the evolution of Romanian Mountain Troops was focused on the specific mountain warfare and thus, in early '90s, there were six mountain Brigades.

The first core Mountain Troops elements, following their re-establishment, gravitated to the 2nd Mountain Brigade around Braşov. Subsequently, to those structures the following were added: the 4th Mountain Brigade, in Southern Carpathians, starting in 1969, the 1st Mountain Brigade, in Northern Romania, starting in 1977, the 5th Mountain Brigade, in Western Carpathians, starting in 1982, the 7th Mountain Brigade, in South-Western Carpathians, in Petroşani area, starting in 1990, and the 61st Mountain Brigade, in Eastern Carpathians, starting in 1991. The Mountain Troops evolution reached its peak in 1991, when there were six large Mountain Troops units, having 15 Mountain Troops Battalions and 6 Mountain Artillery Battalions, being thus an important specialised force:

- 2nd Mountain Brigade, 1964, HQs in Braşov;
- 4th Mountain Brigade, 1969, HQs in Curtea de Argeş;
- 1st Mountain Brigade, 1969, HQs in Bistriţa;
- 5th Mountain Brigade, 1983, HQs in Alba-Iulia;
- 7th Mountain Brigade, 1990, HQs in Petroşani;
- 61st Mountain Brigade, 1991, HQs in Miercurea-Ciuc.

After that, between 1997 and 2006, the 7th Mountain Brigade, the 1st Mountain Brigade, the 4th Mountain Brigade, and the 5th Mountain Brigade were disbanded, one by one, part of Mountain Troops units being re-assigned to the two remaining Mountain Brigades or to other Infantry Brigades belonging to the Romanian Land Forces.

Currently, there are two operational mountain brigades, belonging to the Romanian Land Forces. One is subordinated to the 1st Infantry Division *"DACICA"* (the 2nd Mountain Brigade *"SARMIZEGETUZA"*), and another one subordinated to the 4th Infantry Division *"GEMINA"* (the 61st Mountain Brigade *"GENERAL VIRGIL BĂDULESCU"*).

The 2nd Mountain Brigade is designated to participate in NATO-led operations abroad whilst the 61st Mountain Brigade is designated especially for home defence. Both of them perform their training in a wide range of military operations, from combat operations to stability operations, but, considering their specific design, they are both specialised forces able to carry out actions in rough mountainous terrain and heavy weather conditions.

Just to emphasise the Romanian Mountain Troops experience, it is mandatory to mention that during the past 50 years, the 2nd Mountain Brigade has received the visits of more than 800 foreign military and governmental delegations, from all around the world, delegations that have praised the skills and professionalism of the defenders of the Romanian Carpathians crests.

After 1995, starting with the Partnership for Peace programmes, staff units, companies and platoons within the 2nd Mountain Brigade *"SARMIZEGETUZA"* have trained together with troops from NATO and non-NATO countries (Special Forces and Navy SEALs from the USA, 3rd Commando Brigade from the UK, Special Forces from the Netherlands, Commando Paratroopers from Belgium, Special Forces from Greece and Jordan). A very fruitful cooperation has been also developed, throughout years, with Italian *Alpini* and French *Chasseurs Alpins* within the framework of a lot of training exercises at both staff and platoon levels.

Nowadays, a Mountain Brigade belonging to the Romanian Land Forces has, in its organisational chart, three Manoeuvre Battalions (Mountain Battalions), 1 Mountain Artillery Battalion, 1 Air Defence Battalion, 1 Logistic Support Battalion. As brigade subunits, there are also: Signal Company, Engineer Company, NBC Company, Reconnaissance Company, and Support Company.

Today, mountain troops are able to fight in extremely difficult weather and terrain conditions, and to climb difficult heights and peaks. Moreover, they are excellent shooters, the best in alpine string and long-distance marches in the mountains. The Mountain Troops call themselves *"masters of improvisation"*. They are able to comb the mountainsides on horseback, to conduct combat operations abroad or humanitarian assistance missions, as well as search and rescue missions at extreme heights. The Romanian Mountain Troops may be lacking in very sophisticated equipment and logistic support available to the armed forces of other NATO member countries, but they are able to overcome the disadvantages by employing old-fashioned but still proficient survival skills as well as by thorough training programmes.

The military in the Romanian Mountain Troops have gained a lot of experience in the missions abroad. Thus the troops in the 2nd Mountain Brigade as well as those in the 61st Mountain Brigade have participated, throughout years, in a wide range of missions in Angola, Somalia, Kosovo, Bosnia, Iraq and Afghanistan. In Angola, Somalia and Bosnia, in the '90s, the Mountain Troops participated at platoon level or embedded in other military units. Between September 2005 and March 2007, Mountain Companies from the 21st and 33rd Mountain Battalions were deployed, six-month rotations, in the first mission in Al Basrah area (Iraq) under United Nations Mandate *(UNAMI Mission)*. In Iraq, the Romanian Mountain Troops demonstrated their abilities to act fast and efficiently in any kind of mission in this environment. The main mission of the Mountain Company in Iraq was to provide security in their area of responsibility by patrolling on the main roads, establishing checkpoints, escorting VIPs and convoys, guarding important sites and military bases of the UN mission. During the same period, another Mountain Company from the 30th Mountain Battalion *"DRAGOSLAVELE"* took part in another stability mission abroad, within *ROFND Mission*, in Kosovo theatre of operations, in Gorazdevac area. The main mission of the Mountain Company in Kosovo was to provide security in the area of responsibility by performing all range of peacekeeping specific missions.

Starting in 2007, the 2nd Mountain Brigade *"SARMIZEGETUSA"* Battalions have been involved in missions abroad in the theatre of operations in Afghanistan, on rotation basis. Between 2007 and 2010, this Brigade rotated in the theatre of operations in Afghanistan all its 3 Manoeuvre Battalions. In Zabul Province, which is near Pakistan border, the 2nd Mountain Brigade Battalions provided security and stability in the area of responsibility alongside the American troops deployed in this province.

In general, the battalions had the mission to provide security and freedom of movement on the main highway (that connects Kandahar with Kabul) and the nearby areas and to provide stability in Zabul Province by patrolling between main bases and FOBs (Forward Operating Bases) and performing other missions specific to post-conflict reconstruction operations. The troops in the Mountain Battalions had to deal with many dangerous and complex situations that were specific to this theatre of operations. However, they demonstrated that were very well trained, even though, unfortunately, there were several casualties, killed and wounded in action. In June 2012, the Brigade deployed two Manoeuvre Battalions and a Command element within the framework of an American Brigade, subordinated to RC-South, in Afghanistan, in Zabul Province. Mention should be made that subunits from the 61st Mountain Brigade took part in missions abroad alongside other Romanian Army battalions in the theatre of operations in Afghanistan, starting in 2009, providing company level structures or various OMLT detachments. In all the missions abroad the 2nd Mountain Brigade troops and a major part of the Brigade staff have gained strong operational experience. Considering the identified and learned lessons, the troops belonging to the 2nd Mountain Brigade *"SARMIZEGETUSA"* are able to operate in various environments at high standards.

As all military units around the world, the Romanian Mountain Troops certainly have difficulties but *"Vânatorii de Munte"* always figure a way out. The mountain troops are trained to be independent and to survive in a difficult mountain environment, while conducting their specific missions. They are, for all intents and purposes, part of the Romanian Armed Forces elite. Mention should be made that troops themselves do not easily accept this *"title"*. One of their usual saying is *"We do not call ourselves elite troops or special operations forces, but we like other people to call us that"*. The 2nd Mountain Brigade has had a high readiness level as well as the implicit operational experience, being part of the force package designated to execute NATO-led missions. All its units and subunits have been NATO certified for this kind of commitments. The first phase of the certification process was completed in December 2007. The process continued, according to *CREVAL* provisions.

We cannot conclude the brief *"history"* of the Romanian Mountain Troops without mentioning the fact that they like to think about themselves that they represent perhaps the toughest and the most experienced of the specialised branches, their training being tough, their lives being rough, and their missions complex.

TERRORISM – A CONTINUALLY ACTUAL SCOURGE –

Dr Anelis-Vanina ISTRĂTESCU

The expansion of terrorism at global level represents a reason for great concern as it threatens the security of mankind. New forms of aggression and threat permanently occur and, in order to eradicate them, states have to improve their laws, intensify cross-border cooperation for collecting information on terrorism, and create efficient judiciary mechanisms for the proper punishment of terrorist crimes.

The article approaches terrorism from both doctrinarian and normative perspectives, with a view to reflecting the evolution of the international perception about this destructive phenomenon. Moreover, cyber-terrorism is analysed in correlation with national and international legal standards.

***Keywords**: military affairs; security; terrorism; cyber-terrorism; human rights*

Introduction

Nowadays, we can still feel the effects of the bloody attacks on 11 September 2001, and the resurgence of the phenomenon, under its various facets and meanings, continues to erode the current security environment, where not only the physical confrontation can jeopardise the stability of mankind, but also the one that takes place in the virtual, technological or informational space, with effects on the security of states, in its very substance. The terrorist acts occurred in France in January 2015 and the increase in threats of the same kind in countries previously considered as *"oases"* of security (Belgium, Denmark, Germany) show us how vulnerable we are to this danger whose huge dimension results in not only a state of permanent anguish but also a sense of revolt, coupled with the natural

Dr Anelis-Vanina Istrătescu – assistant lecturer, *"Spiru Haret"* University, Faculty of International Relations, History and Philosophy, Bucureşti.

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

feeling that we must act together and cooperate, because only by an effective and efficient cooperation can we cross the *"abyss"* of the chaos that is about to be installed.

In this labyrinth of terror, cyber security proves to be an imperative element on the list of priorities drawn up periodically by the decision-making factors of the states, in an attempt to provide the governed people with the protection they so urgently need, as an integral part of the social and legal order on which is based any nation governed by the law and the values created around it.

1. The Concept of "Terrorism" between Doctrinal and Normative Views

It is well known that terrorism undermines the force of states, testing their human, material and technological capabilities, as well as the speed of response and adaptability to the new forms of dissemination of terror and panic, based on the extreme fear they are faced with, increased by the helplessness or the impossibility to respond adequately. Terror can occur without terrorism, but at the same time, terror is the key that triggers terrorism[1].

The asymmetry of the war conducted to counteract terrorist acts or facts is precisely due to the fact that the declared enemies of the global order act concertedly and covertly, the state decision-making factors being in various, totally unpredictable situations, which results in casualties or substantial damage, often irreversible. Against this background, thwarting terrorist plans remains the most effective defence instrument of humanity in front of the dangers faced, effective prevention involving the systematic training of personnel with duties in this respect as well as the enhancement of the equipment and facilities used to eradicate a phenomenon whose propagation keeps us in a permanent state of alert.

Terrorism is not only the evil that befalls upon the world, but also the evil coming out of the world, namely our evil, the fanatical part of us and often in us, the obsessive fanaticism of power, of vengeance, of egocentrism, of punishing no matter what, of the purification by killing and destruction[2]. An exhaustive definition of terrorism has not been developed so far, the in-depth research of the concept indicating multiple and highly diverse approaches which are explainable in the context of the vast diversity of its forms of expression; however, from the multitude of definitions given to terrorism, three common elements have been identified

[1] C. Albu, *Arma psihologică – între limite şi performanţe*, Editura Ministerului Internelor şi Reformelor Administrative, Bucureşti, 2008, p. 18, see www.editura.mai.gov.ro.

[2] Gh. Văduva (coordinator) et al, *Terorismul. Dimensiune geopolitică şi geostrategică. Războiul terorist. Războiul împotriva terorismului*, Centre for Strategic Security Studies, Bucureşti, 2002, p. 4.

(use of violence, political objectives, and intention to induce fear in the target population), terrorism being directly influenced by globalisation, a fact that results in the terrorists possibility to move freely in any part of the world as well as to maximally extend the area where they develop their logistic and operative activities, with the consequence of impairing the monitoring operations meant to prevent the spread of this phenomenon[3].

In our opinion, terrorism represents in fact a *"weapon"* used, unlawfully and immorally, for achieving certain political, ideological, cultural or religious goals, by resorting to acts of mass murder, cruelty and extreme violence that flagrantly elude the international law principles, social order rules, religious precepts and moral standards.

If, at doctrinal level, no universally accepted definition has been found yet, at normative level, various domestic and international legal instruments have been adopted concerning the facts considered as acts of terrorism, whose modification has been the natural and inevitable result of not only the changes occurred on the geographical, political and economic map of the world, but also the unprecedented development of technology and information sector. The difficulty of an accurate conceptual delimitation remains even in the normative perspective, as the instruments developed in the area of terrorism at regional or international level are not unitary, covering different fields of social values preservation, protected by the incrimination of terrorist acts and their inclusion in the category of crimes.

After the implementation of the *Convention for the Prevention and Punishment of Terrorism of 1937*, the development of the initial international regulations on fighting against terrorism was marked by the *Resolution no. 303 (XXVII) on 18 December 1972*, adopted by the UN General Assembly, followed by other international legal instruments with deep reverberations into the subsequent strategies for safeguarding peace and security of mankind: *Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents* (1973), *Convention against the Taking of Hostages* (1979), *International Convention against the Recruitment, Use, Financing and Training of Mercenaries* (1989) or *Convention on the Safety of United Nations and Associated Personnel* (1994).

The system implemented by the UN in fighting against terrorism has been improved by the decisions taken at the level of this international body,

[3] For comments in this regard, see M. Atanasiu, F. Repez, *Securitatea şi apărarea ţării în contextul ameninţărilor teroriste*, Editura Universităţii Naţionale de Apărare *"Carol I"*, Bucureşti, 2013, pp. 15 and 18.

either by the General Assembly (Resolutions no. 34/145 in 1979, no. 39/159 in 1984, no. 40/161 in 1985, no. 46/51 in 1991) or by the Security Council of the organisation (Resolutions no. 579/1985, no. 1373/2001, no. 1540/2004, no. 1904/2009). The sustained efforts of the UN towards annihilating terrorism culminated with the adoption of *Resolution on 24 September 2014 regarding threats to international peace and security caused by terrorist acts* (no. 2178/2014), which stipulates, inter alia, the obligation of member states to prevent and suppress recruitment, organisation, transport or equipment supply for people in transit through other countries, to commit, plan, prepare or participate into acts of terrorism. Moreover, member states have the obligation to prevent and suppress providing or receiving training to commit terrorist actions, as well as financing movements or other similar activities, provided that the limitations comply with the conditions imposed by the international norms for protection of human rights, international law of refugees and international humanitarian law.

The international legal framework to suppress terrorism has been simultaneously completed through international treaties adopted in the field of civil aviation security (*Convention on Offences and Certain Other Acts Committed on Board Aircraft* signed in Tokyo, in 1963; *Convention for the Suppression of Unlawful Seizure of Aircraft* signed in the Hague, in 1970; *Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation* signed in Montreal, in 1971) as well in the field of maritime navigation security (*Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation* and *Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf*, both adopted in Rome, in 1988).

Subsequently, the interstate cooperation in the fight against terrorism has been intensified with the adoption of measures aimed at annihilating the financial support for terrorist acts, combined under the UN *Convention for the Suppression of the Financing of Terrorism* in 1999[4], whereby are declared illegal providing or raising funds with the intent to use them or knowing that they will be used to commit crimes in the seizure of aircraft field, unlawful acts against the safety of civil aviation, crimes against internationally protected persons, hostage taking, unlawful acts relating to the physical protection of nuclear material, unlawful acts of violence in airports or against the safety of maritime navigation or of fixed platforms located on the continental shelf, terrorist bombings and acts likely to cause death or serious injury to a civilian or to other person not taking

[4] The New York Convention dated 9 December 1999 was ratified by Romania by *Law no. 623/2002* published in *Monitorul Oficial* no. 852/26.11.2002.

part in armed conflicts, when those facts aim to intimidate the population or coerce a government or international organisation to perform or abstain from performing certain acts (Article 2 of the Convention mentioned).

Strengthening the international legal measures to prevent and combat terrorism was achieved with the implementation of the *International Convention for the Suppression of Acts of Nuclear Terrorism*[5] in 2005, which sanctions the possession of radioactive material or the production or possession of devices, in order to cause death or to produce severe or serious body injuries or damage the property or the environment, as well as the use of radioactive materials or devices. Subsequently, upon adoption, in 2006, by the UN General Assembly, of the *Global Counter-Terrorism Strategy*, was completed the legal framework to eradicate this phenomenon on a global scale.

In Europe, the interstate cooperation materialised by setting up extradition as a form of repression of terrorism for acts expressly covered by Article 1 of the *European Convention on the Suppression of Terrorism in 1977*[6], consisting of crimes committed in the field of aircraft seizure or civil aviation safety, attacks against life, physical integrity or freedom of persons internationally protected, kidnapping, hostage taking and unlawful detention, use of bombs, grenades or missiles, automatic firearm or bomb-letters or parcels, and also for the attempts to commit such facts or for participation in their commission, as author or accomplice.

The revaluation of the legislative priority to firmly fight against terrorism and to redefine the content of terrorist acts required the existence of a new EU treaty to restore legality, embodied in the *Convention on the Prevention of Terrorism* adopted in 2005 by the Member States of the Council of Europe, through which the framework for new policies and interstate preventive cooperation measures was established. The peculiarity of the mentioned treaty is that it considered as terrorist offences the acts incriminated as such in the previous international conventions relating to hijacking aircraft, illegal actions committed in the sector of civil aviation, maritime navigation or against persons under international protection, to which we have referred above.

In Romania, the fundamental legal act that incriminates the crimes of terrorism is *Law nr. 535/2004*[7], amended and completed, by which was implemented

[5] The New York Convention dated 14 September 2005 was ratified by Romania by *Law no. 369/2006* published in *Monitorul Oficial* no. 847/16.10. 2006.

[6] The Strasbourg Convention dated 27 January 1977 was ratified by Romania by *Law no. 19/1997* published in *Monitorul Oficial* no. 34/04. 03. 1997.

[7] *Law no. 535/2004 on preventing and combating terrorism* was published in *Monitorul Oficial* no. 1161/08.12. 2004.

the *National System for Preventing and Combating Terrorism*, in line with the *National Strategy for Preventing and Combating Terrorism*, based on three fundamental principles: *the principle of full legality, the principle of preventing the commission of terrorist acts, the principle of complementarity and coherence in cooperation.*

The events occurred in Europe at the beginning of 2015 marked a turning point in the history of international relations, proving unequivocally that terrorism can affect anyone and can incur at any time, which made the European leaders return to negotiations and be aware of their enormous responsibility to reconsider and implement a new security strategy designed to ensure strong combat of acts of terrorism.

In this context, in the light of the *European Union Internal Security Strategy* approved on 25 February 2010 and the *European Parliament Resolution of 17 December 2014 on the European Union Internal Security Strategy*, was adopted the *European Parliament Resolution of 11 February 2015 on anti-terrorism measures* that amends the substance of the existing legal and institutional framework on terrorism, by the main objectives therein undertaken:

- to effectively settle the issue of *"foreign combatants"*, including in terms of the need to have a harmonised definition of the concept by the Commission, along with the incrimination in the national legislation of member states of the travel to a conflict zone in order to join a terrorist organisation;
- to substantiate and apply an antiterrorism pact with a multi-level approach, which would treat radicalisation, development of cohesion and social inclusion, by promoting religious and political tolerance, counterbalancing online instigation to terrorism, preventing and repressing recruitment into terrorist organisations and employment in armed conflicts, stopping terrorist activities financing and bringing immediately any participants into terrorist actions before judicial bodies responsible for investigating, judging and sentencing;
- to implement the new Schengen evaluation mechanism and adopt directives related to the passenger name record (PNR) and data retention;
- to use the Europol capabilities in a more efficient manner, including its authorisation to identify online extremist or terrorist materials or contents as well as the regulation of an European tracking system related to terrorist financing;
- to improve the efficiency and coordination of criminal justice response through Eurojust, by harmonising the legislation related to the foreign combatants within the EU space and facilitating the cross-border cooperation to collect evidence in terrorist cases;

- to promote a global partnership against terrorism and increase collaboration with the African Union, the Gulf Cooperation Council and the Arab League, and the United Nations Organisation.

The unprecedented expansion of terrorist phenomenon makes us understand that the issue in question cannot be dealt with only at a formal or contemplative level, as it requires a multi-level approach, in which the interest of every nation must be correlated with the interest of the international community and with the need to protect the human being, irrespective of the fact that he/she belongs to a society or another.

2. Approaches to Terrorism in Current International Judicial Practice

The study of the case-law relevant to our research brings to the fore a change of perspective on the active subject of acts of terrorism in international relations area, resulting from the extension of the scope of normative acts undertaken by states at national or international level related to terrorism and military operations. In other words, to understand terrorism, we have first to establish who can be the author, instigator or accomplice of crimes or terrorist acts?

Such a clarification has been recently sought by the Dutch courts that have addressed the CJEU in case C-158/14[8] for reaching a preliminary decision for the EU member states, to establish whether the activities of armed forces during an armed conflict under the international humanitarian law may be considered as terrorist crimes within the meaning of Framework Decision 2002/475/JAI[9] or terrorist acts within the meaning of Common Position 2001/931/PESC[10] and of the EC Regulation no. 2580/2001[11].

The settlement of such preliminary decision by the European Court in Luxembourg shall have major effects on cases subjected to the judgment of certain

[8] The request for the adoption of a preliminary ruling was made by the Dutch Court on 4 April 2014, following an action brought under Article 263 *FTEU*, for the inclusion of an indigenous group (*Liberation Tigers of Tamil Eelam*) on the list covered by Regulation no. 2580/2001.

[9] The request of the Dutch Court related to the Framework Decision of the Council 2002/475/JAI dated 13 June 2002 on fighting terrorism, as amended by the Framework Decision 2008/919/JAI of the Council dated 28 November 2008. According to the Framework Decision, terrorism is a combination of two elements: objective (in terms of criminalised facts) and subjective (in terms of the purpose sought).

[10] The clarification was requested as compared to the Common Position of the Council dated 27 December 2001 on the application of specific measures to fight against terrorism.

[11] The Regulation (EC) no. 2580/2001 of the Council dated 27 December 2001 on the specific restrictive measures against certain individuals and entities in order to fight against terrorism was streamlined by the Regulation no. 610/2010 of the Council dated 12 July 2010, deciding on the implementation of Article 2, para. 3 of the first regulation mentioned.

acts of terrorism by the national judicial bodies of each EU member state, not only in terms of capacity of persons held responsible for such actions (military personnel as well), but also in terms of judicial norms applicable for such cases, issues that have to be taken into account in the military strategies of the future armed conflicts.

Establishing a uniform European case-law in this respect will also have consequences for Romania – an EU member state – whose national legislation relating to terrorism does not contain provisions expressly stipulating that members of the Armed Forces could be investigated, tried and convicted for acts of terrorism, so that the silence of the law can be construed to mean that anyone, including the military, could be active subjects of crimes and terrorist offences. The subject is regulated under Article 4 para. 1-5 of *Law no. 535/2004* relative to prevention and combat of terrorism, as further amended and completed, the content of which explains the notions of *"terrorist entity", "terrorist", "structured group", "terrorist group", "terrorist organisation"*, and also under Article 32-38 of the said Law, where we find the facts considered as terrorist offences, without referring to the capacity of persons whose criminal responsibility may be engaged under the respective act.

The extensive interpretation of the question of law submitted for settlement to the CJEU could lead to the subsequent question whether the acts committed by the military in countering terrorist acts could take, in turn, any form of terrorism. Since the typical antiterrorist *"warfare"* often wipe out any traditional distinction between peace, stability, security and military actions as well as between the actual conflict phase and the post-conflict one, even conducting noble peacekeeping operations can immediately generate controversy when the military have the obligation to respond or to act militarily to restore stability or simply to protect themselves from the violent actions of terrorist groups or networks[12].

The current reality, however, makes us to notice that we are not dealing with the classical antiterrorist warfare but with antiterrorist actions carried out under the *"hybrid warfare"*.

Relating to domestic law, we consider that the military action to prevent and combat terrorism could not be qualified as acts of terrorism, given the specific nature of antiterrorist and counterterrorist interventions within the legal content of which both defensive and offensive measures are included, aimed at diminishing the vulnerabilities of human and material factors, capturing or annihilating terrorists, liberating the hostages and restoring legal order. This is due to the fact

[12] G. C. Maior, *Incertitudine. Gândire strategică şi relaţii internaţionale în secolul XXI*, Grupul Editorial RAO, Bucureşti, 2009, pp. 211-212.

that terrorism fighting strategies are based on the idea of the right to self-defence. What should be emphasised is that military interventions to suppress terrorism will be subsumed, in all cases, under the *principle of legitimacy of using the military force*, as well as the exigency of *proportionality with its purpose*, and especially under the *requirement of respect for human rights*; on the contrary, the responsibility of the military factors committing damaging infringements might be involved. Moreover, the principle of ensuring fundamental rights and freedoms of the individuals also emerges from previous documents adopted at international level, of which it would be sufficient to mention Resolution no. 1373/2001 of the UN Security Council, by which the member states were requested to take appropriate measures in compliance with the international human rights standards (para. 3, f), or Resolution no. 60/158 in 2005 of the UN General Assembly on the protection of human rights and fundamental freedoms in the context of anti-terrorism fight (para. 1, 3, 5, 7 and 10).

The question remains open as to the settlement of case C-158/14 by CJEU and to what extent the opinion of the court will impose the completion and harmonisation of Romanian legislation applicable to the acts or facts of terrorism committed in the course of military operations or armed conflicts.

Equally decisive for the legal order in the space of the European Union will be the decision of the Court of Justice of the European Union regarding the conditions related to the exclusion of persons participating in terrorist organisations or convicted for terrorist acts, from the category of refugees or persons who require further action for international protection, such an issue being the subject of the case brought before the European Court registered under no. C-573/14 and initiated at the request of Belgium[13]. The case to which we refer raises two essential aspects: on the one hand, it calls for clarification of the scope of Directive 2004/83/EC dated 29 April 2004[14], so as to determine whether the elimination of international protection depends on the pre-existence of a judicial convicting decision for terrorist acts provided by the Framework Decision 2002/475/JAI of the Council on 13 June 2002 or it can be decided even in the absence of such judgement, in those cases in which there are reasonable suspicions

[13] The request for a preliminary ruling was submitted on 11 December 2014 by the Council of State in Belgium.

[14] The Directive specified refers to the minimum standards to be fulfilled by a person belonging to another state or a stateless person to obtain the refugee condition or another form of international protection. Pursuant to Article 14, para. 4 of the Directive, states can revoke, terminate or refuse to renew the refugee status of a person, if there are strong reasons to believe that he/she is a threat to the national security or if, following a conviction for a serious offence, he/she is a real danger for the community of the respective state.

for acts of terrorism regarding the applicant calling for protection; on the other hand, CJEU has the power to analyse and explain the scope of the acts of terrorism regulated by the Directive no. 2004/83/EC referred to above, by relating to the purposes and principles of the UN, which will bring noticeable changes in the European judicial perception about terrorist acts in terms of investigation, prosecution, trial and punishment thereof.

We believe that such clarification from the Court becomes imperative, and in consideration of the demands of systematisation related to the protection of human rights, for the mere suspicion of terrorism not to turn into a pretext to commit abuses or to apply unjustified restrictions to persons being in a real need to obtain international protection. Moreover, the standards related to international protection conferred on persons suspected of terrorism have been recently addressed by ECHR, too, into its case-law, of which we could mention the judgment given in *case Husain (Abu Zubaydah) against Poland*[15], whereby the court from Strasbourg found the respondent state responsible for violating the right of the claimant not to be subjected to torture or inhuman or degrading treatment and his right to freedom and security guaranteed by Article 3 and 5 of the European Convention on Human Rights, violations produced following the imprisonment of the victim in a secret prison in Poland belonging to the CIA, the use of inhuman interrogation techniques and the facilitation of the extradition to other CIA secret detention centres, exposing him to the risk of being subjected to other inhuman treatments.

ECHR decided, among others, that the responsibility of public authorities of the states that are parties to the Convention would be engaged, not only for direct violations of the conventional provisions previously referred to, but also when the bodies of the state would tolerate or allow such violations on the territories falling under their jurisdiction. Equally, the decision of the European Court is a form of warning for state leaders concerned with the annihilation of the terrorism phenomenon, determining them to realise that nobody is exempted of liability when violating laws or committing certain abuses, under the pretext of preserving security, as such actions would be, in their turn, real acts of terrorism. The decision mentioned becomes thus, a benchmark of the jurisprudence of the state authorities involved in the collective work to eradicate terrorism, whose prompt and efficient combat does not relieve of the responsibility for practices incompatible with the principle of respect for human dignity, around which any civilised nation gravitates.

[15] The Decision given by ECHR on 24 July 2014 in the case no. 7511/13 became final on 16 February 2015.

We note, in essence, that the suppression of terrorism cannot serve as a justification ground to harm the individual rights and fundamental freedoms, so that between the imperative to maintain local, regional or global security and that concerning the protection of individuals suspected of terrorism, one has to identify a fair balance, a relationship of proportionality based on the theory of the rule of law in a democratic society. Although the dilemma *action vs. inaction* will continue to fuel debates related to the military actions to combat terrorism, members of the armed forces will have the duty to permanently correlate the strategic need with the need to protect the human being, starting from the assumption that man is the central figure of the Universe, whereby the primary objective is to comply with the law and to respect the values protected by its enacting.

3. Cyber Terrorism – A Form of Contemporary Terrorism

The boom of technological development in recent years has made terrorism take on a new form, more dangerous and insidious, manifested in cyberspace, where the success in identifying the author is obstructed by the virtual camouflage and the weapons used do not have anymore a conventional nature specific to those used in theatres of operations, but rather to a *"war of ideas"* in which *information* becomes the stake of the battle. Cyber terrorism has therefore become the new tool to undermine the security of humanity, whose continuous metamorphosis requires the utmost vigilance and increased speed of response from the state authorities called to respond to this challenge launched by those for whom terror dissemination is based on manipulating information and its illicit use, by various methods, such as viruses introduced into computer systems, electronic jamming mechanisms, use of skilled agents, launching direct attacks, hiring hackers to take control of servers belonging to strategic bodies or institutions, unauthorised access into computers and destruction of databases.

Cyber terrorism can be regarded as an overlap between two elements, which represent the greatest fears of mankind and which have evolved since the end of the last century: cyberspace and terrorism – escalation of violence on civilian targets and suspicion on computer technologies[16]. Cyber terrorism has already had a fast and extremely worrying growth rate, concerning not only the Internet

[16] A. Barbu, *Cyberterorismul – viitorul terorismului?* in *Perspective privind guvernanţa securităţii internaţionale*, coordinated by M.M. Neag, Editura Academiei Forţelor Terestre *"Nicolae Bălcescu"*, Sibiu, 2012, p. 175.

networks but also certain unparalleled attacks to neutralise the decision-making elements *("decapitation strikes")* of a target organisation, cross-border and transnational, consisting in attacking the database of the management systems and especially the nuclear, biological and financial security systems of the structures which a terrorist organisation considers optimal for the achievement of its interests, in any part of the world[17]. The scope of the phenomenon as well as its unpredictable and uncontrolled expansion has compelled states to identify and develop programmes and strategies to fight against cyber terrorism and to regulate, in terms of legislation, the necessary framework for the suppression of this new use of terror within the virtual environment.

At European level, normative and institutional instruments have been created in order to suppress cyber crime, and in this respect, the *Convention of the Council of Europe on Cybercrime of 2001*[18] was adopted, which defined the concepts of *"information systems", "computer data", "service provider", "traffic data"* and incriminated four categories of crimes: *crimes against confidentiality, integrity and availability of data and information systems* (illegal access, illegal interception, affecting data integrity, affecting the system integrity, abuses on the devices); *cybercrimes* (cyber forgery, cyber fraud); *crimes relating to contents* (information related to child pornography); *crimes related to the violation of intellectual propriety and related rights.* By the subsequent Additional Protocol of 2003[19] incriminating racist and xenophobic acts committed through computer systems, this convention was completed, by explaining the expression *"racist and xenophobic material"*, and indicated to the signatory states the task of incriminating, in the domestic law, several categories of crimes: *distribution of racist and xenophobic materials by computer systems, the insult based on a racist and xenophobic motivation, the denial, gross minimisation, approval or justification of genocide or of crimes against humanity.*

Constant efforts towards the annihilation of cyber terrorism have also been made in recent years by the bodies of the EU, materialised in documents of tremendous importance, such as the *Resolution of the European Parliament on 25 November 2009*, by which the EU member states were called to cooperate to create a comprehensive strategy to combat cybercrime, to establish a specialised department of the EU

[17] For comments in this regard, see I. Pentilescu, *Dinamica terorismului informaţional, Revista Forţelor Terestre* no. 1/2009, http://www.rft.forter.ro/2009_1_t/07-arm/03.htm.

[18] Adopted in Budapest on 23 November 2001, the Convention was also ratified by Romania by *Law no. 64/2004* published in *Monitorul Oficial* no. 343/20.04.2004.

[19] Additional Protocol dated 28 January 2003 was ratified by Romania by *Law no. 105/2009*, published in *Monitorul Oficial* no. 278/28.04.2009, stipulated that the provisions of Article 5, para. 1 of the Protocol on the insult being based on a racist and xenophobic motivation were not applicable.

to provide support in case of identity theft and identity forgery, and to clarify the rules of competence and the legislative framework applicable in cyberspace.

The initiative of the European legislative body was not fruitless, being followed by the establishment, in 2012, of an intervention team in case of computer emergency (CERT-EU), and culminating, in 2013, with the development of the *Cyber Security Strategy* of the European Commission and the EU High Representative for Foreign Affairs and Security Policy, in which there were proposed as priorities, freedom and openness, enforcement of norms, laws and values protected by the EU in the cyberspace too, development of the cyber security capabilities, enhancement of international cooperation in cyberspace[20]. Within the EU there are countries like Denmark, which has not only adopted a purely defensive position against cyber threats, but has also managed to establish offensive cyber warfare units vested with the power to launch their own cyber attacks in order to paralyse the enemy air defence, electricity and water supply systems as well as the essential web sites[21].

Romania has also joined the states involved in the actions of response to cyber terrorism, not only by ratifying international specific treaties and conventions or applying in the domestic practice certain fundamental principles acknowledged at regional or global level, but also by enacting and applying its own normative instruments aimed at ensuring domestic judicial and social order, so stringent in the current security environment. In this regard, we could mention, for example:

➢ *Government Emergency Ordinance no. 98/2010 on the identification, designation and protection of critical infrastructures*[22], which stipulates the measures and the procedure related to the identification and designation of national/European critical infrastructures and the assessment of the need to improve their protection, in order to increase the capacity to ensure the stability, security and safety of socio-economic systems and the protection of persons;

➢ *Government Decision no. 494/2011*[23], which establishes the Romanian National Computer Security Incident Response Team (CERT-RO)[24], within which the Early Warning System and Information in Real Time on Cyber Incidents is established;

[20] See http://eeas.europa.eu/policies/eu-cyber-security/index_en.htm

[21] See http://www.juridice.ro/354695/danemarca-va-crea-o-unitate-de-razboi-cibernetic-ofensiv.html.

[22] Published in *Monitorul Oficial* no. 757/12.11.2010.

[23] *Ibidem*, no. 388/02.06.2011.

[24] By Order no. 1062/19.10.2011 of the Minister of Communications and Information Society published in *Monitorul Oficial* no. 34/16.01.2012, CERT-RO was designated the national body for approval, verification and control, as well a body of analysis, assessment and intervention in the field of cyber security.

➢ *The National Strategy for Critical Infrastructure Protection*, approved by Government Decision no. 718/2011[25], which brings clarification on the concepts of *"vulnerability", "risk factors", "threats", "states of danger", "aggressions"*, applicable in the area of critical infrastructures, and provides strategic objectives, principles, actions to be taken, as well as the implementation, monitoring and evaluation mechanisms to ensure the protection sought;

➢ *The Memorandum of Understanding between Romania and the Council of Europe on Combating Cybercrime* signed on 15 October 2013, by which the new office of the Council is established in Bucureşti, having responsibilities in the field of combating cybercrime;

➢ *The Memorandum of Understanding between NATO Cyber Defence Management Board and the Romanian Intelligence Service on Cooperation in the Field of Cyber Defence,* approved by Government Decision no. 144/2013[26], the memorandum being aimed at implementing the new strategic concept of NATO and placing defence against cyber threats among the priority actions of the Alliance;

➢ *Romania's Cyber Security Strategy* and *Action Plan at National Level on the Implementation of the National Cyber Security System* approved by Government Decision no. 271/2013[27], acts based on which the National System for Cyber Security (SNSC) coordinated by the Operative Council for Cyber Security is established;

➢ *Norms on 21 October 2014 on Protection of Nuclear Installations against Cyber Threats*[28] approved by Order no. 181/21.10.2014 issued by the President of the National Committee for the Control of Nuclear Activities.

Despite the multitude of secondary legislation, at present, in Romania, the issue of cyber security is partially regulated by special laws, therefore existing such provisions in Title III on the prevention and fighting against cybercrimes of *Law no. 161/2003*[29] *on certain measures to ensure the transparency in exercising public positions, public functions and in the business environment, preventing and sanctioning corruption,* where we can find both the explanations of some expressions, such as *"information system", "automatic data processing", "computer program", "computer data", "security measures"* (Article 35), and the crimes criminalised and sanctioned by the law: crimes against confidentiality and integrity of data and computer systems (Article 42-46), cyber crimes (Article 48-49), child pornography crimes by information systems (Article 51).

[25] Published in *Monitorul Oficial* no. 555/04.08.2011.
[26] *Ibidem*, no. 283/20.05.2013.
[27] *Ibidem*, no. 296/23.05.2013.
[28] *Ibidem*, no. 803/04.11.2014.
[29] *Ibidem*, no. 279/21.04.2003.

We consider that the law mentioned contributes to guaranteeing the social values protected thereby, but it is lacking and even obsolete as compared to the new types of crimes occurred in the virtual space, bearing in mind that it does not create the institutional, procedural and logistic mechanisms for optimising the methods and means of fighting against cyber terrorism in its current forms.

On the other hand, *Law no. 286/2009 on the New Criminal Code of Romania*[30] entered into force on 1 February 2014, as further amended and completed, includes in Title VII, Section VI, *crimes against the safety and integrity of cyber systems and data*, where the following facts are incriminated and sanctioned by the criminal law: illegal access to a cyber system (Article 360), illegal interception of cyber data transfer (Article 361), alteration of the integrity of cyber data (Article 362), disrupting the operation of cyber systems (Article 363), unauthorised transfer of cyber data (Article 364), illegal operations with computer devices or programs (Article 365).

The analysis of the existing Romanian legal system makes us note that Romania will not be able to adequately and efficiently fight against terrorism in the cyber space, in the absence of a special law of cyber security in line with the realities of our time, able to comply with the requirements imposed by our country membership of NATO, UN, EU and OSCE, to allow full integration into the political and military structures created to preserve security and to reach the level of performance of the other states with which it interacts in the judicial, political and military field. The controversies and debates built around this subject still bring to the fore intense discussions between the promoters and opponents of the *Law on Cyber Security of Romania,* declared unconstitutional by Decision no. 17/2015[31] given by the Romanian Constitutional Court, which established that the normative act under examination was vitiated in its entirety. This decision of unconstitutionality was preceded by other previous decisions of the Court, by which were declared unconstitutional three laws with effects in the field of combating terrorism, so that judicial norms of tremendous importance in the antiterrorist fight undertook by Romania at both national and international level became ineffective.

First of all, we take into account the *Decision of the Constitutional Court no. 1258/2009*[32] by which was declared unconstitutional the *Law no. 298/2008*[33] *on the storage of data generated or processed by the electronic communication service*

[30] *Ibidem*, no. 510/24.07.2009.
[31] *Ibidem*, no. 79/30.01.2015.
[32] *Ibidem*, no. 798/23.11.2009.
[33] *Ibidem*, no. 780/21.11.2008.

providers for public or by public communication networks, as well as for amending the *Law no. 506/2004 on processing personal data and protection of private life in the sector of electronic communications*. In the grounds of the mentioned decision, it was found, in essence, that the law in question did not comply with the precision requirement inherent to all normative acts, brought unjustified limitations to the exercise of the right to private life and secret correspondence, affected the right to free communication or expression and it did not meet the condition of proportionality considered a benchmark principle in the case-law of the ECHR.

The second decision with effects on the legislative field under research is the *Decision no. 440/2014*[34], by which the Constitutional Court established the unconstitutionality of *Law no. 82/2012 on the storage of data generated or processed by the electronic communication public networks providers and by the electronic communication services providers for public*, as well as on the amendment and completion of *Law no. 506/2004*[35] *on processing personal data and protection of private life in the field of electronic communications* and of Article 152 of the Criminal Procedure Code.

The decision of the Constitutional Court was based on the grounds mentioned in its decision on the unconstitutionality of *Law no. 298/2008* to which we referred above as well as on the arguments evoked in the *Judgment given by CJEU dated 8 April 2014*, given in the joint cases *C-293/12 – Digital Rights Ireland Ltd against Minister for Communications, Marine and Natural Resources and others and C-594/12 – Karntner Landesregierung and others*. It is to be mentioned that the Luxembourg Court decision directly invalidated the Directive 2006/24/EC of the European Parliament and of the Council dated 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or public communications networks and amended the Directive 2002/58/EC, due to the fact that it violates Article 7, Article 8 and Article 52 para. (1) of the Charter of the Fundamental Rights of the European Union, as it affects the right to private life and the right to have protection of personal data in terms of the requirement of proportionality which should exist between the measures applied by public authorities and the public interest pursued.

The third decision with implications in the legal field on cyber terrorism is the *Decision no. 461/2014*[36], by which the Constitutional Court found

[34] *Ibidem*, no. 653/04.09.2014.

[35] *Ibidem*, no. 1101/25.11.2004.

[36] *Ibidem*, no. 775/24.10.2014, the decision in question was adopted by majority of votes, with the separate opinion of three judges, according to whom the provisions of the law examined were constitutional, in respect of the obligation related to the registration of the prepaid cards users

the unconstitutionality of the Law on the amendment and completion of Government Emergency Ordinance no. 111/2011 on electronic communications, in relation with the provisions of Article 1 para. (5), Article 26, Article 28, Article 30 and Article 53 of the fundamental law, ascertaining the applicability *mutatis mutandis* also in this case, the arguments on which was based the adoption of its previous decisions no. 1258/2009 and 440/2014 related to the unconstitutionality of *Law no. 298/2008* and of *Law no. 82/2012*. In addition, following the control exercised, it was decided that the new law did not meet the clarity and predictability requirements of any legal provision, as it was fully able neither to clarify the scope of persons in charge of data collection nor to establish whether such persons would have the task of ensuring the confidentiality, security and use of data, which would create the premises of committing abuses to the detriment of the private life conferred to beneficiaries of electronic communications services; on the other hand, it was ascertained that, although the law examined extended the scope of persons obliged to identify the users of electronic communications services, it did not provide the guarantees for the exercise of the fundamental rights conferred to such users, as it did not stipulate the express obligation of those who registered and stored personal data to ensure their confidentiality.

Returning to Decision no. 17/2015 mentioned above, by which the Constitutional Court declared as unconstitutional the Law on Cyber Security of Romania, we consider that the urgent adoption of a new law complying with the principles evoked in the grounds declaring the incompatibility of the law with the Constitution of Romania should be more than a priority for the Romanian legal power, since the delay in the regulation of the judicial framework necessary to combat cyber terrorism does nothing but allows the proliferation of this phenomenon, the increase in the criminality in this area and also the exposure of Romania to an extremely high vulnerability to the security risks which the European countries face. In the absence of a legal instrument that should enable combating and especially preventing cyber terrorism, the risk of terrorist acts in the virtual environment grows exponentially, placing Romania on the map of the countries deprived of the means of defence and of the legal armoury, indispensable to an effective and appropriate suppression of this scourge that affects the security of mankind.

Among the deficiencies found by the Constitutional Court, which substantiated the decision on the ineffectiveness of the normative act on the repression of cyber-terrorism, were included, inter alia: the failure to comply with the precision

and the identification of users of Internet services, in consideration of the fact that it was not justified the application of a different legal regime among prepaid cards and Internet services users and telephone services subscribers who were registered and identified, according to the law.

and predictability requirements of any normative act, regarding the legal text on the scope of the rules applicable to the cyber infrastructure users and the type of data to which access is allowed for incidents occurring in the cyberspace (threats, cyber-attacks or incidents), and also regarding the assessment of the relevance of requested data; the absence of regulation concerning the manner in which the data are actually accessed; the imprecision of the conditions on notification of risks and cyber incidents to the authorities designated for this purpose (CNSC, CERT-RO, ANCOM or other authorities) without establishing the circumstances that are required to place the notification and the content of such notifications, including data that should be disclosed; the absence of any express provisions to ensure that persons affected by the documents issued or acts committed while applying the law have the possibility of addressing an independent and impartial court to challenge the administrative acts that impose certain obligations and responsibilities upon them and affect their legitimate rights or interests; the failure to regulate the competencies on the control and monitoring of all holders of cyber infrastructures and to clarify the procedures for monitoring and control, as well as the procedures for finding and punishing the offences.

After analysing the express grounds set out by Romania's constitutional body by Decision no. 79/2015, we herewith submit the following *de lege ferenda* proposals, whose implementation in the forthcoming national cyber security law would give remedy to some of the shortcomings identified by the Court and lead to the development of a normative act in full compliance with the fundamental law of the state, rule of law, rules of democracy and fundamental human rights and freedoms:

❖ **the establishment by the law of a special department on cyber security issues within the Directorate for Investigating Organised Crime and Terrorism (DIICOT)**, consisting of specialised prosecutors, empowered to conduct investigations, prosecute and send offenders to justice for cyber terrorism crimes, to work together with the Romanian Intelligence Service, the National Computer Security Incident Response Team (CERT-RO), the Operative Council for Cyber Security and the Office of the Council of Europe on Fighting against Cybercrime; the department concerned would operate within the current service for preventing and fighting against acts of terrorism and those against state security within DIICOT, which would require the reorganisation of the current service for preventing and fighting against cybercrime, to avoid overlapping competences in the same field or in related fields; establishment of certain specialised structures in cyber terrorism field should be harmonised with the provisions of *Law no. 508/2004* on the establishment, organisation and functioning within the Public Ministry of the Directorate for Investigating Organised Crime and Terrorism, which would involve assigning specialised police agents and officers as well as recruiting highly skilled cyber specialists;

❖ **regulating a clear procedure regarding the conditions for monitoring the users of cyber infrastructures, the access to personal data of those users and the terms in which could be decided limitations in the exercise of their right to private and family life and of freedom of expression**, by correlating the forthcoming law on cyber security with the provisions of Article 154 of the Criminal Procedure Code of Romania on the preservation of computer data; the provision to which we refer provides the necessary conditions for the preservation of computer data stored, the competent authorities to apply such measures, the maximum period of application of the measures, the document based on which it can produce effects and its compulsory elements, stipulating the obligation of public electronic communication networks providers or electronic communication service providers to preserve cyber data and to ensure their integrity and confidentiality, obtaining prior authorisation from the judge of freedoms and rights relating to transmission of preserved data and their collection and the term during which the judge would rule on the request for transmission of data submitted by the prosecution bodies, establishing the obligation to communicate to the person prosecuted a written notice about his/her data retention;

❖ **the insertion into the forthcoming Romanian law on cyber security of a certain provision introducing the right of persons affected by this law to address to a court** to challenge the administrative acts that may affect their rights and interests and to obtain reparation for the prejudice thus caused; we consider that, in such cases, the new normative act should establish the jurisdiction of the Section for Administrative and Tax Contentious within the administrative and tax tribunals where the alleged facts occurred; we have hereby considered the correlation with Article 1 para. 1 and Article 10 of *Law no. 554/2004 on Administrative Contentious* and the terms to have the benefit of the rights covered by Article 11 of this law; even if the unlawfulness of the measures ordered by the court in the proceedings of criminal prosecution of cyber terrorism would be challenged, we believe that the rule of the future law on cyber security should regulate the procedure for the settlement of such complaint with respect to the conditions stipulated by Article 336-341 of the Code of Criminal Procedure, firstly, by challenging the measure before the Prosecution Office investigating the case or the superior Prosecution Office and, subsequently, before the Criminal Department within the Court of Appeal, where it is located, so as to be taken into consideration jointly with the provisions of Article 40 of *Law no. 535/2004 on Preventing and Combating Terrorism.*

The proposals of *de lege ferenda* referred to above are not exhaustive but may serve to create an appropriate legal framework to prevent and combat cyber terrorism, as the absence of a law in this field dramatically increases the power of terrorists, who continue to organise and orchestrate new attacks into the cyberspace, with unpredictable and irreversible consequences on national stability and security. The area where terrorism mainly develops consists of countries with poor governance, facing ethnic, cultural or religious tensions, economically underdeveloped or having permeable borders[37]. That is why drafting a special law on cyber security will help to strengthen the state mechanism aimed at ensuring the safety of everyday life and eliminate the state of anxiety provoked by terrorists, creating the means of effective protection of the governed people. The difficulty of identifying the best legal solutions depends on the ability of the public authorities to anticipate the new forms of aggression in the cyber space, precisely because terrorism is in itself a complicated machinery, a latent process[38].

We can conclude that the adoption of a new law on cyber security, consistent with the constitutional principles and fundamental human rights, represents a high-priority objective, which the Parliament, the Government and all other decision-making factors involved in the field of maintaining peace and social order must acknowledge and deeply understand, making them act urgently, now when any country might become a terrorist target.

Selective Bibliography

1. *Convention of the Council of Europe on Cyber Crime of 2001.*
2. *Decision of the Constitutional Court of Romania no. 17/2015.*
3. *European Parliament Resolution of 17 December 2014 on Renewing EU Internal Security Strategy.*
4. *Global Counter-Terrorism Strategy of 2006.*
5. *European Union Internal Security Strategy of 2010.*

[37] C. Barna, *Terorismul, ultima soluţie?*, Editura Top Form, Bucureşti, 2007, p. 11.
[38] J.L. Marret, *Tehnicile terorismului*, Editura Corint, Bucureşti, 2002, p. 70.

CONSIDERATIONS ON THE INFLUENCE VARIOUS TYPES OF LEARNING AND TECHNOLOGY EXERCISE OVER MODERN EDUCATION MECHANISMS

Major Dr Dragoş BĂRBIERU

Alongside classical training forms and methods, eLearning proves to be of great help, especially with the use of personalised study materials in interactive formats. Moreover, as the author points out, eLearning methods and techniques allow for saving time and money as trainees can achieve their tasks anywhere they have access to a computer and Internet connection. In addition, eLearning can accommodate different learning styles. As for trainers, eLearning poses a series of pedagogically, technologically and eventually pragmatically driven challenges. Yet, when facing new challenges, new requirements and educational necessity, one needs more than technology and pedagogy can offer, namely new energies and new aspirations.

***Keywords**: eLearning; education; pedagogical approach; advanced distributed learning; learning styles*

Education between Theories and Approaches

The development of new technology, the low price for the current ones, and the diversification of teaching methods lead to high educational performance but these are not enough criteria to guarantee a learner's preparation. The learner-related education is an intimate[1] process that is connected to a series of attitude generating actors, which we will try to highlight based on the impact they have. Such actors are not independent, so classifying them based on importance is a matter of personal choice. The main actor is the environment where the individual spends most of his/her time, namely the family. The family is the one that can design requirements and criteria, the one that can promote values and establish goals. The individual

Major Dr Dragoş Bărbieru – *"Carol I"* National Defence University, Bucureşti.

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

[1] The Romanian pedagogy researcher Constantin Narly considers that education is *"both a social and an individual act, simultaneously"*.

is another actor, represented by the personal effort and individual work, the interest manifested in gathering and managing new pieces of information. Educational goals, individual career plans and curiosity represent important elements for such an actor. The innate intellectual gift can enhance the personal effort and it is the element that develops the range of individual choices. In the current socio-economic context, where the pragmatic aspect based on competences is emphasised to meet the requirements of an ever changing society, the necessary education to successfully integrate an individual in a society does not surpass the capabilities of a common individual. The only requirement is that the individual should get the necessary information timely by triggering the factors that enhance the desire to learn and know.

To this end, the debates between the approaches to development offered by psychologist Jean Piaget[2] and the mental universal representations that support their innate character in Noam Chomsky's view[3] raise a series of questions about the educators's role, the author stating that the environment does not introduce more complexity inside someone's brain than in other organs[4]. There have been different trends of thought in the history of education, theories about the ontogenetic process and the influences of various endogenous and exogenous factors. The heredity[5] theory focuses on the important role of genetic factors and it is sceptical about the teacher's environment and role. There have resulted various theories out of the previously mentioned one, some of them being criticised and others denied, as such: the inneist theory, the organicist, the sceptical, and the racist theory, similar to Cesare Lombroso's[6] theory of the innate criminal. Biologist Jean-Pierre Cahngeaux[7] states that *"the extreme structural complexity of the central nervous system is in contrast to the weak genetic information quantity available"*. Radu Gologan, the leader of the Romanian Mathematical Olympiad team and the President of the Mathematical Sciences Society makes the following comments in an article[8]: *"...there has not been any child from the rural area to come to the national mathematical contest. Referring to the grades 5 to 12 where there were 700 children*

[2] The youth are not miniature adults, ignoring the own ways of representing lives.

[3] Noam Chomsky considers that language is a cognitive specialised system with psychological and neurological representations.

[4] Noam Chomsky, Jean Piaget, *Teorii ale limbajului. Teorii ale învăţării*, Editura Politică, Bucureşti, 1988, p. 335.

[5] http://en.wikipedia.org/wiki/Jean-Pierre_Changeaux

[6] http://en.wikipedia.org/wiki/Cesare_Lombroso

[7] http://en.wikipedia.org/wiki/Jean-Pierre_Changeaux

[8] http://www.hotnews.ro/stiri-esential-15644874-problemele-esentiale-din-educatie-vazute-ong-uri-gradinita-obligatorie-calitatea-profesorilor-plu-ultimii-2-ani-olimpiada-nationala-matematica-nu-ajuns-niciun-copil-scoala-sateasca.htm

from across the country, we must say there was no child from the rural area". This way the focus is laid on the environment where the upbringing takes place and, more than that, on the role the school has. Yet, we cannot draw general conclusions as in this situation the rationale should work based on exceptions from the general rule. To support this, the book *Bell Curve* written by Richard Herrnstein and Charles Murray is an attempt to demonstrate that intelligence is the dominant factor within an individual's line of life and it is based on a series of statistics about the socio-economic status. This subject will be always controversial, in the author's opinion, and we should state that environment is a catalyst factor in an individual's shaping.

As a reaction to the hereditarian theory, the ambientalist theory stresses the importance of the socio-cultural environment and the exogenous factors. J.B. Watson states that any child can be transformed in any type of adult provided one has the needed tools: time, patience and the sum of rewards and punishments given. Behaviourist theories have not yet vanished from education; they are met even today within the *"red spots"* when national standardised tests are administered. The curiosity of children and their endless energy are often prevented from manifesting by such methods. Throughout the human species evolution, curiosity has been the mechanism by which humans have tried to know, helping them to synthesise and approach things in an abstract way, to deal with concepts, to approximate in order to anticipate dangers and new situations. When they are at the beginning of the road, children use this resource fully, in order to build themselves a personal perspective on reality. We believe that this functionality diminishes and eventually fades away when we speak about an adult that has an already built perspective on the world, as the adult can approach things in an abstract way, he can anticipate, and this issue can question the lifelong learning concept. We should not yet mistake a repetitive activity that renders pleasure, satisfaction and rewards for the curiosity that surpasses the area of a single field or activity. We believe that the promoters of the behaviourist theory have very well understood that pain and sorrow bring people together, as people are equal when facing them, while happiness seen as accomplishment is a state that is different from one person to another.

The theory of double determination reconciles the different perspectives of the two theories already mentioned and also introduces education as a main factor. Lev Vygotsky's social constructivism states that the learning process can be achieved through models, in a social context: *"We know ourselves as we are aware of the others and we are aware of the others as our own awareness about our self* *comes from the awareness the others have about us"*[9]. This theory has had a special influence and the concept web 2.0 supports it. That is why web 2.0 is not a really new technology; it is more of a mentality. The characteristics of the web 2.0 are embedded in the social and interactive aspect. Models can influence the way, while by means of interaction and imitation we can reach our goals. The value of this theory can be seen in informal education. The multitude of media channels, blogs and forums, virtual conferences, social media, Massive Open Online Courses[10] confirm the individuals desire to learn, to communicate, to be connected and participate. In formal education, most of the eLearning platforms have software eLearning tools to communicate and bring interaction among students. A necessity for students is the presence of the tutor, of various means to communicate, of an access to various educational resources using mobile devices. We thus state that social interaction and the social aspect of learning can lead to conformism and uniformity. Moreover, they call for authority, overvaluing the teacher's role, which can limit the critical spirit and curiosity, the student having some patterns and predefined recipes. It is hard to believe that the tutor/teacher can meet the educational needs for a large group of students on his own, and that is why the student-centred learning process, focused on the student's needs tries to involve the other students in the class in a real exchange of ideas and knowledge. The birth of this theory gets intersected with the Russian revolution, Vygotsky being influenced by Marxism, so we can anticipate the birth of the *"new man"*, educated and influenced by society, while there is no accent on the unique and particular nature of the individual.

Competency-based Education

Today, the media of communication and information can exploit human's social nature via different means, which is possible responsible for Vygotsky's success. Competency-based education is a challenge for teachers as well, as they have to adapt to the labour market requirements, therefore their competency area must be permanently updated. Should we anticipate, we believe that the development of the artificial intelligence along with the progress in the fields like nanotechnology and neuroscience will change both the teacher and the school. The former one could be replaced with software intelligent programs that address each individual separately based on own needs and that do not depend on a lot of other factors like emotions, fatigue, time etc. We consider that the history of education has kept

[9] Emilia Albu, *Psihologia vârstelor*, Universitatea Petru Maior, Tg. Mureş, 2007.

[10] http://en.wikipedia.org/wiki/Massive_open_online_course

school connected to the real knowledge keepers and generators. At the beginning, education addressed the elite, school being active alongside temples, churches and monasteries. The Enlightenment and the Industrial Revolution were the factors that brought education to the public level, it thus becoming a necessity for the society modernisation. The public mandatory education becomes a state attribute. In Romania, since the first Romanian school in Braşov[11] that was coordinated by St Nicolas Church and the first modern law of the Romanian education[12] that was issued during Cuza reign education has passed through various stages and the results have not been sudden. In this regard, school was managed by the church, various court administrations, and it was much later when the public mandatory education was introduced. We mention such historical events in order to explain what has led to competency-based education. Gradually, various specialisation programmes have been introduced in schools, based on various technologies[13], this aspect making possible for students to enter the labour market without much further ado. Excepting the states national educational or research projects and also some disciplines that fit in the services field as occupational areas, a synchronisation between school and the economic environment has been needed. It is thus possible that the state would not be the main actor in the future and might lose the role it had in the 20th century, that is to educate people on a large scale. The economic system shows that among the knowledge generator vectors are the large companies and corporations. The European research projects represent, in our opinion, an attempt to save the traditional school by bringing and orienting the academic community towards new technologies, interests, directions and societal challenges. The economic model is the one generating these changes and for sure significant alterations will occur in the future. It is considered that, by introducing competences, social cohesion level will increase, enhancing the graduates' opportunity to find and fill a work position, knowing that youth unemployment for people between the age of 18 and 24 is currently high in Europe[14]. We consider that only by introducing competences filling new positions will not be enhanced, as the main factor is the lack of jobs and not the quality of education, knowing that many companies provide various internships and training to their newly hired employees.

[11] The first Romanian school was established in Braşov, at St Nicholas Church, in Şcheii Braşovului neighbourhood, in 1583.

[12] The Law on Education in 1864.

[13] Cisco programme can be an example.

[14] http:// ec.europa.eu/eurostat/statistics-explained/index.php/file:employment _rates_by_age _group, 2013.

Contemporary Theories of Learning

Contemporary learning theories establish four learning types[15].

Cumulative learning is characterised by acknowledging new patterns of thoughts, where the information is new and has no connection to what we have previously learned. This type of learning best fits to the multiple-choice tests, where the main focus is on memorising. Using the eLearning LMS (learning management system) and the software tools offered by this would help considerably in cumulative learning. We can thus imagine several situations, such as: new terminology learning (NATO terminology) or a new program running rules, a game like Virtual Battlespace 3 etc.

The introduction of multiple choice tests in the secondary and tertiary education is a good thing; the drawback is that these tests do not scaffold logical thinking, synthesis and analysis, and even more, they limit imagination. An essay, a synthesis, a composition, the logical and coherent solution found to a math problem will always be thresholds for the learner whose knowledge is built on multiple choice tests. Needless to say that less desired are the situations when a faulty rationale can lead to a right answer, situations that can be possible. Leaving aside the wrong answers and choosing the most possibly correct answer in a multiple choice item is another aspect that is detrimental to learning. It goes without saying that the multiple choice test is output oriented and it does not matter how one gets to it. Introducing multiple choice tests in the development stage as a form of evaluation and checking for the secondary school represents a limitation as they are not aimed at developing and testing judgemental synthesis, analysis and transfer skills. This is the context where one can meet students that cannot be rational and deductive, cannot develop ideas or analyse a given text. It is even worse sometimes when the student can know the answers for some series of sets of tests within an exam, being motivated towards memorising instead of focusing on correlations between the acquired pieces of information.

In educating and training adults into acquiring certain terminologies, concepts, information where one needs to know and memorise without performing complex analysis, the multiple choice test is a facile solution. To this end, in order to encourage the students attending online courses within the *Advanced Distributed Learning Department*, the multiple choice final test can be performed twice. The final test does not contain a fixed set of questions, as they are generated randomly from a huge pool of questions. This way, each student has a personally tailored quiz at the end of the course, with various sets of questions displayed each time the test taker tries to complete the course. This method is used at the *European*

[15] Knud Illeris, *Teorii contemporane ale învăţării*, Editura Trei, Bucureşti, 2009, p. 31.

Security and Defence College[16], where the students have endless trials to be able to complete the course by the trial and error system. The final goal is not to differentiate, rank or eliminate but to get each learner achieve the desired set of knowledge in a given timeframe. The meaning of the word *test*[17] most frequently met is about connotations which identify themselves with the results of the participants to lead to ranking both people and results and establishing a hierarchy for those who pass the test, while the *test* itself is a mere check on the knowledge level, as the tested people do not competing to fill a certain position.

The same vision is followed in the German Armed Forces where the trainer plays a crucial role in educational and training programmes, providing knowledge and developing skills. Moreover, the trainer has other responsibilities such as: ensuring educational and training programme quality – the activities in the online programme are connected to real-world applications, ensuring that the distributed learning programme schedule is respected, and providing support for students in case of questions and technical problems.

Assimilation learning represents the type of learning where the individual connects between what he is currently learning and previously inherited patterns. Although the topics within the subject matter follow a logical line from simple to complex and enhance assimilation learning, we still believe that the Romanian school does not focus on pluridisciplinarity and multidisciplinarity, interdisciplinarity and transdisciplinarity. Currently, school does not promote interdisciplinary and transdisciplinary aspects, such as the link between the numerical system and geometry, the correlation between Kirchhoff's laws and geophysics, similarities and differences between the birds and humans migration. The existence of higher mathematics within some disciplines makes the understanding of some phenomena impossible, while the lack or the insufficient attention paid to logics changes the student's perception in a negative way. The skill of correct thinking is one of the most essential elements that will positively mark individuals' lives as this is a necessary but not sufficient condition to make the best decisions. We consider that any exam should include a test to check the logical process of thinking. This model is used in Romania for the judicial system entrance examination[18] and there are also similar tests in other countries to allow access

[16] The European Security and Defence College LMS is hosted by Romania at the *"Carol I"* National Defence University, accessible at https://esdc.adlunap.ro

[17] Test (according to DEX) is a stage when perceptive skills are examined, be they kinetic or mental, intellectual development, aptitudes etc. Also, a test is a written or oral form of knowledge examination. An exam is a way to test and appreciate the knowledge a student or a candidate gets in order to complete a course or get a position.

[18] *Guide to Solving the Logical Thinking Evaluation*, issued under the project *Technical Support to Provide Critical Thinking Tests*, financed by the World Bank programme for the judicial reform, see http:// www.uvt.ro/files.

to a master programme. GMAT test, for example, focuses on critical reasoning, analytical writing assessment, quantitative, sentence correction, reading comprehension, integrated reasoning[19]. Moreover, our opinion is that extending the curricula on a longer period of time would be counter-productive. A connection between the cumulative and assimilation learning as well as the methods proposed for rapid learning are offered by Tony Buzan[20].

Learning by accommodation or transcendent learning means breaking some patterns of thought and acquiring some new ones to correspond to new learning contexts. The individual must accept something different and this fact is more complicated than adding new information to an already existent pattern. In a society where information is accessible by various sources, where the pace of scientific discoveries is alert, an inflexible thinking is an obstacle into adapting an individual to the environment. It is by experience that we have reached a new perspective, which is the probability-based thinking, where one can associate probability factors to events and information. Placing new knowledge into a cognitive flow and into a specific context can offer a larger perspective on the world. This pattern of thought should build the pattern that is closest to the contingent reality. The cognitive flow is based on the logical argumentation and its placement into a context refers to experience and imagination. A software tool that is very useful in this case is Mind Mapping, useful for creating representations of mental maps. We have to say that learning is not a singular act, entailing emotions as well. That is why an inflexible mind can generate negative and frustrating attitudes. Generally, individuals notice what they like or what they understand, and that is why breaking the patterns of thought, represented by this type of learning, is energy-consuming, yet there is the bonus of *"….this type of learning that is characterised by the possibility of being reactivated and applied in many different relevant contexts"*[21].

The main threshold for this type of learning is conformism, because once a pattern of thought is created, it will generate comfort for all our actions and we will try to eliminate any new idea that changes the current state. Were we to consider the book *Thinking, Fast and Slow* written by psychologist Daniel Kahneman[22] it should be stated that here we meet the pleasure of cognitive ease: *"The link between the positive emotion and cognitive ease of System 1*[23] *has a long evolutionary history"*.

[19] http:// www.edventure.ro/engleza/gmat.

[20] http://en.wikipedia.org/wiki/Tony_Buzan.

[21] Knud Illeris, *A Comprehensive Understanding of Human Learning*, p. 32.

[22] http://ro.wikipedia.org/wiki/Daniel_Kahneman.

[23] Psychologist Daniel Kahneman, Nobel Laureate, considers that human thought is controlled by two systems, system1 that he calls *thinking fast* , which is intuitive, unconscious and does not need

Transformational learning is another learning type that is deep and vast. This can bring changes in personality, being the result of a crisis situation. Professor Jack Mezirow launched this concept in 1978 in an article published in the US journal *Adult Education Quarterly*. The author considers that *"the two major elements of transformational learning are, firstly the critical reflection or self-reflection over any assumption – critical evaluation of the sources, nature and consequences of our mental habitudes – secondly, our free and full participation in a dialectical discourse to validate the best reflexive argumentation"*. The need to build a new inner vision of the world, in a world where the valid information is not always easily accessible, the critical spirit and sceptical nature turn the individuals that hint for this kind of education into rejected or unreliable individuals. To us, the final target of this endeavour should be a higher level of understanding, but it could be possible that negative/positive feelings accompany us on the way. Were we to take a short imagination test, where a third party told us that all we know, all we learned or were told by others is false, we could assume it to be a traumatising experience. Transformational learning can be the ultimate level in the process of becoming a mature adult. Should we parallel the transformational learning stages to intelligence development stages belonging to Jean Piaget and Chomsky's inneist perspective we could state that it is only at certain stages of life that we can access the transformational learning and that it is a certain genetic determinism for that. Simultaneously, not all individuals feel the need to know, and those who do not have such curiosity have other types of needs that could change their way of living, their habits, their values. Critical thinking is not easily accepted by individuals, groups, ideologies, and that is why the end of the critical thinking father, Socrates, a spring of unlimited thoughts for humanity, to the benefit of the state, came the way it did. The method he used, maieutics, targeted reaching truth via dialogue and debates, where the principle of ignorance and doubt in his discourse had a deeply critical character.

Stephen Brookfield[24] is an objector to the transformational learning and his arguments are based on ideological criteria. He sees critical reflection as a criticism of an ideology, stating: *"...it focuses on people's adjustment to become aware of the way capitalism moulds systems of beliefs and assumptions (ideologies) that justify and maintain social and economical inequities"*[25]. We consider that critical thinking should be no one's enemy, as this is meant not to bring one injustice

voluntary effort or control, while system 2, called *thinking slow* is conscious, it uses deductive rationales and it needs a lot of effort.

[24] http://www.stephenbrookfield.com/Dr_Stephen_D._Brookfield?Home.html

[25] Jack Mezirow, *A General Approach over Transformational Learning,* p. 177.

but, on the contrary, to connect one to a brighter light, to a contingent reality, in order to rebuild and progress. The main target for this type of learning is not related to ideologies. From a constructivist perspective, it is considered that personal evolution means going through certain stages that all lead to maturity. Maria Carmen Matei (Ştefănescu)[26] states that *"a transdisciplinary perspective, like the one advanced by critical thinking, can ensure a better awareness of the dysfunctional phenomena (disinformation, diversion, discrimination, manipulation etc.) and yet a better defensive strategy against these, keeping control over their detrimental effect on the quality of life as much as possible"*.

Society and family, with the help of the values they promote, school and its contribution, via the quality of educational performance, are actors that work together and should not be taken separately in the act of human education. Research in the field considers heredity to be an important actor as well, yet, without degrading it, we consider that the Romanian educational system should address the many common ones and not the few chosen. Currently, the undergraduate educational system abounds in series of negative aspects relating to family relationship degradation due to the fact that parents no longer spend time with their children, being either very busy or abroad, to work. Moreover, most students are graded based on unreal criteria.

The need for critical thinking has come, in our opinion, as a current of thought against the abundance of information overlapped with the individual's confusing attitude towards society. Should we look at the abstract of the doctoral thesis *Decizia socială din perspective gândirii critice*[27] the idea of introducing critical thinking in schools and universities curricula is highlighted, arguing that *"students can be taught minimal critical thinking terms in any field. There is basically no reason why students should not use the basics of critical thinking they learned in a subject and then to extend this information (with limitations, of course) to other subjects and fields they study"*.

The community can substantially contribute to individuals' informal education and a new actor emerges on the stage, where the technological support can make possible a large array of open courses, libraries, forums, blogs, Wikipedia, communication/information platforms and open educational resources[28].

[26] Doctoral thesis, *Raţionarea în contextul gândirii critice*, see http://www.unibuc.ro/studies/Doctorate 2014iulie/MATEI

[27] Mircea Florian Ionescu, Doctoral thesis *Decizia socială din perspective gândirii critice*, Bucureşti University, Faculty of Philosophy.

[28] Open educational resources are educational and research materials accessible in any environment, in the public domain or under creative common law, which is they can be used freely, adapted, distributed and redistributed by others without restrictions or under limited restrictions, see Ovidiu Voicu, *Resurse educaţionale deschise: Oportunităţi pentru România*.

This is a concept firstly defined in 2002, within UNESCO meeting in Paris, aiming at integrating software technologies and educational resources along with promoting scientific research, to offer free access to all of them for teachers, students as well as for those that are not necessarily and formally enrolled into a form of the educational process.

Education must address everybody, it must keep standards for evaluation and examination by putting an end to the multiple-choice tests run within entrance examination, selection process, ordinary exams, national exams; thus, prosperity and security will be accomplished. Developing capabilities to adapt and think can replace lack of experience for the young graduates. Introducing informal logic and critical thinking in schools would be a huge advantage. Supporting disadvantaged children, integrating the Romany people, stimulating the educational staff into performance, programmes and frequent contacts between school and family can be clear courses of action.

Using open resources requires well protected information systems. In this regard, all educational materials that can be accessed on the Internet regardless of the chosen security solution must be unclassified.

E-Learning in the National Defence University

Without pretending exclusivity, *eLearning* provides new educational and training opportunities since it is popular today in all universities, being a side component of the traditional learning, based on hardware and software technologies brought up by the evolution in society. This form of information dissemination can be extremely effective if the military personnel who need training are scattered on a large geographical area, in different theatres of operation. *ELearning* as a concept and as a means to disseminate knowledge is part of the *Advanced Distributed Learning* concept[29].

"Carol I" National Defence University currently organises military courses via the *Advanced Distributed Learning Department* and grants a certificate of accomplishment, supporting teaching activities for the master and doctoral programmes. The success of this type of training is also proved by the large number of graduates. Thus, for *Introduction to NATO* course, there have already been 23 series, for the *Conflict Management and Negotiation* course, there have been 15 series, for *Law of Armed Conflict* course, there have been 12 series, for *Common Security and Defence Policy* course, there have been 10 series, totalling an average of 8,000 student accounts in the department's *learning management system – LMS.*

[29] The e-learning programme *(TADLP – The Army Distributed Learning Program)* was initiated in 1998 being part of the US military training and development system.

Besides the achievement of resource savings, the trainee can have own learning pace, no time restrictions, while he/she is off duty, without putting aside his work assignments. He/She can achieve the tasks anywhere, around work, family and friends. To reduce confusion and alienation while learning, various forms of communication offered by the *eLearning* platform can be used, to turn learning into a more social activity. However, technology does not offer solutions to identify the test taker in an evaluation process and neither does it cover the reliability of the fact that the test taker simultaneously refers to references while being evaluated.

A huge advantage for the military personnel is the introduction in the Romanian Armed Forces of qualification courses that are certified by *ANC (National Qualifications Authority)*. These courses are carried out with the support and online technology through the online e-learning platform of *"Carol I"* National Defence University. Courses such as health and safety at work, environmental manager, PSI technical personnel provide new qualifications and skills useful for both military and civilians.

Through using the e-learning system, the military personnel will gain access to a modern and high quality educational system, designed for the specific needs of the area, which is available anytime and anywhere with minimal costs.

BIBLIOGRAPHY

1. Noam Chomsky, Jean Piaget, *Teorii ale limbajului. Teorii ale învăţării*, Editura Politică, Bucureşti, 1988.

2. Knud Illeris, *Teorii contemporane ale învăţării*, Editura Trei, Bucureşti, 2009.

3. Daniel Kahneman, *Gândire rapidă, gândire lentă*, Editura Publica, Bucureşti, 2012

4. ***, TRADOC Pamphlet 525-8-2, *The US Army Learning Concept*, see www.tradoc.army.mil

STAFF OFFICERS TRAINING ABROAD (1878-1940)

Colonel (r.) Dr Petre OTU

The study analyses the methods of training staff officers abroad in the period between the War of Independence and the Second World War. The phenomenon depended to a large extent on the culture and civilisation model followed by Romania in the particular period. The staff officers who were trained abroad played an important role in the modernisation of the Romanian military body, occupying positions of great responsibility such as ministers of war, chiefs of general staff, commanders of army corps and divisions, directors or professors at the Superior War School as well as noted military theoreticians. Among them we can mention Alexandru Averescu, Grigore Crăiniceanu, Constantin Christescu, Leon Mavrocordat, Constantin Prezan, Constantin Iancovescu, Alexandru Iarca.

***Keywords**: Triple Alliance; Germany; France; Carol I; Superior War School*

The modernisation of the Romanian society began, as it is known, in the mid-19th century, the Forty-Eighters project being the matrix of the extremely complex process. The model lying at the root of the reforming activities in the Romanian Principalities outside the Carpathians, and then in the modern Romanian state, was one of Western origin, bearing the French or German mark. However, in time, some aspects of the modernisation process were criticised. In this context, it is well known the concept of *"Forms without Substance"*, theorised by the *"Junimea"* Society, especially by Titu Maiorescu, its mentor and leader, whose scope and depth were evident. The Romanian society and state firmly followed the path to modernity. However, they preserved some characteristics usually encountered on the outskirts of large areas of civilisation[1].

Colonel (r.) Dr Petre Otu – Institute for Political Studies of Defence and Military History, the Ministry of National Defence.

[1] For further details regarding Romania's modernisation see: Gheorghe Iacob, Luminiţa Iacob, *Modernizare-europenism (România de la Cuza-vodă la Carol al II-lea), vol. I, Ritmul şi strategia modernizării, vol. II, Percepţie, trăire, identitate*, Editura Universităţii *"Alexandru Ioan Cuza"*, Iaşi, 1995; Daniel Barbu, *Bizanţ contra Bizanţ. Explorări în cultura politică românească*, Editura Nemira, Bucureşti, 2001; Dan Berindei, *Modernitate şi trezire naţională. Cultura naţională română modernă. Studii şi eseuri*, Editura Fundaţiei Pro, Bucureşti, 2003; *Istoria Românilor*, vol. VII, tome II, *De la Independenţă la Marea Unire (1878-1918)*, coordinator Gheorghe Platon, Editura Enciclopedică, Bucureşti, 2003; Ioan Saizu, *Modernizarea României*

The evolution of domestic military structures was part of the same civilising and modernising paradigm. The armies of the two principalities, established in 1830-1831 and improved by different rulers, were transformed by Alexandru Ioan Cuza into a national army following the French model. Carol I of Romania enhanced it in terms of organisational structure, equipment and staff training, so it was able to participate with respectable results in the Russo-Ottoman War in 1877-1878, known by the public as the *"War of Independence"*.

During his long reign, Carol I tried to replace the French organisation and functioning model with the German one, considering the fact that, starting October 1883, Romania became a member of the Triple Alliance, which was the main security vector of Romania up to the First World War[2]. Carol I efforts were partially successful and, during the world conflagration, especially after Romania entered the war, in August 1916, alongside the Entente, the French model was very important. Moreover, between 1916 and 1918, a French military mission led by General H.M. Berthelot was operational in Romania.

In the interwar period, Romania was part of the French European security system, which was directly reflected in the construction and functioning of the country's military apparatus. In 1924, the Romanian Armed Forces officially adopted the French military doctrine that was in force until the outbreak of the Second World War[3].

*

An important aspect of the Romanian military system modernisation between 1878 and 1940 was the enhancement of the staff structures. Officers were trained to man the structures in peacetime and at war. Their establishment was an expression of the administrative-bureaucratic revolution imposed by the increase in the number of armies as well as by the technical developments in the 19th century.

contemporane (perioada interbelică). Pas şi impas, Editura Alfa, Iaşi, 2003; Horia Roman Patapievici, *Discernământul modernizării. 7 conferinţe despre situaţia de fapt*, Editura Humanitas, Bucureşti, 2004; Florin Ţurcanu (coordinator), *Modelul francez şi experienţele modernizării. Secolele XIX-XX*, Institutul Cultural Român, Bucureşti, 2006; Sorin Radu, *Modernizarea sistemului electoral din România (1866-1937*), Institutul European, Iaşi, 2007; *Schimbări şi devenire în istoria României. Lucrările Conferinţei internaţionale "Modernizarea în România secolelor XIX-XX",* Cluj-Napoca, 21-24 May 2007, coordinators: Ioan Bolovan, Sorina Bolovan, Cluj Napoca, 2008; Constantin Schifirneţ, *Formele fără fond. Un brand românesc*, Comunicare.ro, Bucureşti, 2007 etc.

[2] *Documente Diplomatice Române, seria I, vol. 11, 1883*, volume by Alin Ciupală, Rudolf Dinu, Antal Lukacs, Foreword by Mihai-Răzvan Ungureanu, Minister of Foreign Affairs, Introduction by Rudolf Dinu, Editura Academiei Române, Bucureşti, 2006; see also G. Căzan, S. Rădulescu-Zoner, *România şi Tripla Alianţă*, Editura Ştiinţifică şi Enciclopedică, Bucureşti, 1979.

[3] For further details regarding the evolution of the Romanian military body see also: Petre Otu (coordinator), *Reforma militară şi societatea în România (1878-2008*), Editura Militară, Bucureşti, 2009.

The particular bureaucratic structure was a French initiative, but those who enhanced it were the Prussians (the Germans). The Prussian General Staff was established by Gerhard Johann David von Scharnhorst (1755-1813) at the beginning of the 19th century, and enhanced by Field Marshal Helmuth von Moltke (1800-1891) and then by Alfred von Schlieffen (1833-1913) in the second half of the same century. By that time, staff officers did not enjoy special appreciation, being considered simple bureaucrats, deprived of contact with the troops and the realities of the battlefield. Moltke transformed them into an elite, highly trained group, being also put on probation in combat units. Thus military management was significantly improved, the German victories in the wars with Denmark, Austria and France being the result of the enhanced bureaucratic instrument too.

It was also Moltke and his successors who contributed to the Great General Staff special status that worked independently from the central military administration structure, namely the Ministry of War (Defence). The former was in charge of preparing the armed forces for the war, as well as of studying the hypotheses and operations plans, while the latter was responsible for providing the armed forces with everything they needed[4].

In Romania, as it is well known, the first staff structure, namely the Staff Corps, was established by Alexandru Ioan Cuza on 12/24 November 1859. Following the War of Independence, the Romanian staff structures enhanced to adapt to the changes in the international arena. In this context, it was very important the Decree no. 2945 on 29 November/11 December 1882, through which the Armed Forces Great General Staff was established. Subordinated to the Ministry of War and staffed by specially trained officers, it was responsible for the problems related to the military organisation and the armed forces preparation for war. Moreover, it studied the armed forces of different states, designed and updated the map of the country. On this basis, the War Depot was transformed into the 3rd Section of the Great General Staff. The following step was represented by the *Law on the Staff Service*, promulgated by Decree no. 808 on 6/18 March 1883, through which the old *"Staff Corps"* was disbanded and the staff service for the entire army was organised[5].

[4] Fernand Schneider, *Histoire des Doctrines Militaires*, Presses Universitaires de France, Paris, 1964, p. 59.

[5] For further details regarding the evolution of the Great General Staff see: *Istoria militară a poporului român*, vol. V, Editura Militară, Bucureşti, 1988; *Apărarea naţională şi Parlamentul României*, vol. I, Editura Militară, Bucureşti, 1992; *Istoria Statului Major General Român. Documente 1859-1947*, Editura Militară, Bucureşti, 1994; Petre Otu, *Statul Major General şi reformele organismului militar 1878-1916*, in *Statul Major General 1859-2004. Istorie şi transformare*, Centrul Tehnic-Editorial al Armatei, Bucureşti, 2004, pp. 46-64; Ion Giurcă, Maria Georgescu, *Statul Major General Român (1859-1950). Organizare şi atribuţiuni funcţionale*, Editura Militară, Bucureşti, 2012.

*

Following 1878, for about a decade, staffing the Great General Staff and its structures was one of the thorniest problems of the Romanian military construction in the late 19th century. Up to 1883, staff officers were educated and trained abroad, but their number was so small that the growing needs of the Romanian Armed Forces could not be met. Education and training in the country was a desideratum, though, up until that date, there had been some concerns for the establishment of a specialised institution in the field. We mention, in this context, the initiative of General Ioan Emanoil Florescu, who, on 18 March 1872, received Carol I approval to establish a War Academy, where courses should last for three years. The decree was not implemented because of the lack of funds, and General Florescu departure from the Ministry of War (1876) as well as the outbreak of the Russo-Romanian-Ottoman War postponed the project *sine die*.

Another initiative was that of 1881, when the staff officers educated and trained abroad took the initiative of establishing a local Superior War School, obtaining the first share of 33,000 lei of the funding for its organisation. In January 1882, Colonel Eraclie Arion was appointed Director, and the law in 1883 stipulated the establishment of the Superior War School directly subordinated to the Great General Staff[6].

The Superior War School was established on 8/20 August 1889, through Decree no. 2073, studies lasting for two years. On 4/16 November 1889, the first regulation on the newly established institution was adopted. The establishment of the Superior War School was a necessity. It gradually became the main institution to educate and train staff officers. Mention should be made that, in 1894, the Ministry of War decided to send a small number of officer candidates and officers abroad to keep *"our training up to date with that abroad"*[7]. The decision was generally respected and, until the First World War, were educated and trained 417 officers in the country and only 19 abroad. The decision was primarily motivated by budgetary reasons. However, we consider that the authorities of that time committed an error. The need to highly train staff officers abroad and the contact with the expertise of those countries in the field were partially counterbalanced by practice periods performed by officers of different specialities in the Austrian-Hungarian and German Armed Forces.

[6] *Istoricul Şcolii Superioare de Război 1889-1939*, Bucureşti, 1939, pp. 31-32.

[7] General-locotenent Mircea Agapie, maior Dănuţ-Mircea Chiriac, maior Ion Emil, maior Constantin Hlihor, *De la Şcoala Superioară de Război la Academia de Înalte Studii Militare. Comandanţi, profesori, absolvenţi (1889-1895)*, Editura Academiei de Înalte Studii Militare, Bucureşti, 1995, p. 11.

The procedure of sending officers, including staff ones, to study abroad entails going through some compulsory stages, included in the Regulation on sending officers to study abroad and in the orders issued by the minister of war. Typically, the ministry negotiated with the foreign partner the number of candidates and the conditions of participation and then published the notice about the organisation of the competition in *"Monitorul Oastei"*. It was open to all who met the criteria set by the authorities in the country with the foreign partners.

The government and the ministry sought to provide the legal framework for the officers training, especially in Germany and Austria-Hungary, members of the Triple Alliance, Romania was also part of. In this regard, the convention with the two countries, approved by King Carol I on 12/24 July 1898[8], was of particular importance. The goal of such an action was *"to complete and improve the training"* of officers in terms of the *"front service"*. The conditions discussed with German and Austrian-Hungarian partners and agreed by the emperors of the two empires were as follows:

➢ Admission of 12 officers for a two-year practice period in the Austrian-Hungarian Army every year. The practice period began on 1 October, the Romanian officers taking part in all the front activities alongside their Austrian colleagues. When the practice period was over, they returned to their units in the country.

➢ Six other staff officers were admitted in the Austrian-Hungarian Army to perform staff service in regiments, also taking part in the annual manoeuvres of the Austrian-Hungarian Army. The activity began on 1 January, the practice period lasting for ten months.

➢ Every year, six candidate officers were admitted in the Prussian Army to perform the military service for a three-year period. They took part in all the military activities alongside Prussian officers. Each series of six officers comprised four infantry candidates, as well as one artillery and one cavalry candidate. The activity began on 1 October each year.

➢ At the Artillery and Engineer School in Charlottenburg, two officers were admitted annually. Education and training lasted for two years, the Prussian military authorities deciding, for each case, if the officers could continue the practice period or not.

➢ The costs related to supporting the Romanian officers to be educated and trained in the Prussian Army were covered by the Romanian Government.

➢ The young Romanians were engaged in Prussian regiments following a special order issued by the King of Prussia, and they performed the service according to the rules existing for Prussian citizens.

[8] Romanian Academy Library, Department of Manuscripts, Dimitrie A. Sturdza Archive, XIII, varia 6; see also XIII, varia 1.

Emphasising the great importance of the agreement between the two governments, the Romanian Prime Minister at that time, liberal D.A. Sturdza, stated: *"I think, Sire, that the thorough implementation of these provisions will be very useful for our military training. Thus, our officer corps,* D.A. Sturdza continued, *will have the opportunity to know closely and in the most favourable front service conditions two of the great European powers, to get familiar with the responsibilities related to the officer position there, as well to the troops training and command, according to an as perfect as possible military organisation requirements"*[9].

D.A. Sturdza also pointed the fact that a rigorous selection of those who were to be sent to the two armies was necessary, as the Romanian Army superior interests were at stake. Therefore, he considered that *"any condition related to personal favour should completely disappear, and only the real, serious, and well assessed qualities of the candidates should be taken into account to decide whether they are worthy to be entrusted with such an important mission"*[10]. Among the qualities and conditions, the Prime Minister mentioned the following: perfect health; good look; loyalty, sincerity and honesty; exemplary behaviour in the barracks and outside them; serious military skills; knowledge of German; single.

Throughout their stay in Germany and Austria-Hungary, the officers were monitored by the Romanian diplomatic agents in Berlin and Vienna. In his report to the King, the Prime Minister insisted on the idea that the pay and accessories of the officers in training in the two countries had to be sent regularly and in the amount stipulated by the German legislation. Moreover, he required that the officers to be selected should enhance their German language knowledge.

D.A. Sturdza considered the convention very important as, within five years, the Romanian Army would have 74 officers educated and trained that way, and within a decade, their number would increase to 200.

On 25 August 1898, D.A. Sturdza sent a telegram to Berlin to inform Alexandru Beldiman that King Carol I approved all the proposals regarding sending Romanian officers to be educated and trained in Germany and Austria-Hungary. He asked the Romanian minister to thank the German authorities and to clarify, within a reasonable period, the problems related to the pay and accessories of the officers that were to come to study[11]. An identical telegram was sent to Emil Ghica, Minister of Romania to Vienna.

One month later, Alexandru Beldiman informed the Ministry of Foreign Affairs about the norms established by the Prussian military authorities for those admitted

[9] *Ibidem.*

[10] *Ibidem.*

[11] *Ibidem*, XIII, varia 7.

to study. Throughout the period they were in the Prussian Army, they had to obey the Prussian laws and regulations but they did not become Prussian citizens. The exams were taken under the same conditions as the Prussian candidates. However, after graduation, they could not be appointed to military or civilian positions in Prussia. In the case of marriages with German women, the emperor consent was necessary. The Romanian young officers practically became Prussian officers during the period they were educated and trained in the two military institutions and units.

Given the rules, Beldiman informed that the Legation had limited responsibilities regarding monitoring the candidate officers who studied in Germany. Its role was to take note of the opinions expressed by the responsible military authorities and to ensure that the money expected to be sent to Germany arrived to the military units in time[12].

The convention concluded by the Romanian and German Governments was very clear as far as the status of the Romanian candidate officers in the Prussian Army was concerned. They became Prussian officers, pledged allegiance to the Emperor and obeyed the military and civilian legislation in Germany.

Based on the convention, Romania sent the first group of officers in Germany, in the autumn of 1898. It consisted of: Constantin Lăzărescu, Constantin Oprescu, Mihail Todicescu, Mihail Buttescu, George Athanasescu, Anton Gh. Vasilescu[13].

The convention was in force up until 1908, when it was not renewed by the authorities in Bucureşti, as it was difficult to reintegrate the Romanian officers who were educated and trained in Germany. Up until that time, 67 officers belonging to different services and specialities were trained in the Austrian-Hungarian, German and Belgian armed forces. Nearly half of them were prepared in the field of staff. However, the practice of sending officers to be educated and trained in the armed forces of the two countries continued up to the First World War.

Starting in 1908, the Ministry of War decided to annually send two officers to study in Bulgaria and in the Russian Empire.

Although the number of the staff officers educated and trained abroad up until the First World War was small, their contribution to the development of the Romanian Armed Forces, its command and staff structures, was highly important.

Firstly, most of them were professors at the Superior War School in Bucureşti, and some of them commanded it for a certain period of time. Among them, Alexandru Averescu, Leon Mavrocordat and Constantin Christescu can be mentioned.

[12] *Ibidem*, XIII, varia 8; Mihail Buttescu, *Vânătorii Reginei Elisabeta*, Gheorghe Vartic edition, Editura Militară, Bucureşti, 2012.

[13] *Ibidem*, XIII, varia 3.

Secondly, the staff officers educated and trained in France, Germany, Torino and Brussels were promoted to higher ranks, commanding large units and high commands. Therefore, during the First World War, some of them, such as Generals Dumitru Iliescu, Constantin Prezan and Constantin Christescu were chiefs of the General Staff, while others were part of the command of the armies, army corps and divisions.

Thirdly, the officers educated and trained abroad considerably boosted the development of the Romanian military thinking, as they published studies and papers or managed some military publications[14]. According to the Romanian Academy statistics, in 1914, in Romania, there were 20 military publications, 300 political publications, 86 economic publications, 54 juridical, 38 scientific, 37 literary, 30 religious and didactical, 8 geographical and historical, 8 humanistic ones[15]. Some of them were managed by officers educated and trained abroad, while others had such officers in their editorial boards.

In the interwar period, the staff officers training abroad continued in the war schools in Paris and Torino. There were 57 officers trained (49 in Paris and 8 in Torino). Such a measure was justified as the Romanian Armed Forces were based on the French doctrine. Officers were usually sent abroad after graduating the first year at the Superior War School in Bucureşti, their number amounting to 2-3 annually. They were selected from the first ten officers of the series of graduates that particular year by the director of the institution.

If we compare the number of the graduates from the Superior War School in Bucureşti between 1919 and 1940, which amounted to 457, without considering the Quartermaster Branch, to the number of the staff officers trained abroad, the percentage of the latter is almost 12.5%.

Conclusions

Staff officers training represented an important direction as far as the Romanian military body between 1878 and 1940 was concerned. In the first decade after gaining independence, training was performed abroad, and after the establishment of the Superior War School, it was performed mainly in the country.

Up until the First World War, training abroad was performed in education institutions in Italy, Germany, France, Belgium and Austria-Hungary. In the interwar period, destinations were France and Italy.

[14] See details in Petre Otu (coordinator), Teofil Oroian, Ion Emil, *Personalităţi ale gândirii militare româneşti*, vol. II, Editura Academiei de Înalte Studii Militare, Bucureşti, 1997, 2001.

[15] Ion Bulei, *Arcul aşteptării 1914.1915.1916*, Editura Eminescu, Bucureşti, 1981, p. 180.

1889-1914	
War School in Torino	8 officers
War School in Brussels	4 officers
War School in Paris	3 officers
War School in Berlin	3 officers
War School in Vienna	1 officer
1919-1940	
War School in Paris	49 officers
War School (Institute) in Torino	8 officers
Total	**76 officers**

Officers who graduated from the war schools abroad (1889-1940)

No.	Branch	Number of officers
1	Infantry	35
2	Navy	16
3	Artillery	12
4	Medicine	10
5	Cavalry	7
6	Technical Officers	6
7	Engineering	4
8	Geodesy	4
9	Veterinary	2
10	Administration	1
Total		**97**

Distribution of the officers educated and trained abroad by branches

Between the War of Independence and the Second World War, the azimuth of the staff officers training was the West, the Romanian Army adopting, up to 1914, mainly the German model (better to say a composite model), and starting in 1916, the French model (in full).

The contribution of the staff officers trained abroad to the Romanian Armed Forces modernisation process was very important, the majority of them being appointed to high commands or the command of tactical, operational or strategic large units or units (divisions, army corps, armies or group of armies) during the two world wars in the 20th century. Moreover, they contributed, through their literary and journalistic activity, to the enhancement of the staff officers training in the country.

There was another characteristic of the Romanian military structure evolution. Up until the First World War, the Romanian military were educated and trained mainly according to the German military doctrine spirit and provisions. However, between 1916 and 1918, they fought against the former ally, having French trainers, alongside the Russian Army up to its disintegration, in the autumn of 1917.

In the interwar period, education and training were performed in accordance with the French doctrine. However, between 1941 and 1945, the Romanian Armed Forces fought alongside the German Armed Forces and, after 23 August 1944, against them. Clearly, such paradigm shifts fully required the Romanian Armed Forces command and staff structures skills and competence.

Staff officers educated and trained abroad (1878-1940)

Name and surname	Highest rank	Highest position	Educational institution (period; country)
Andronescu Mihail	Divisional General	Second in Command, 6th Territorial Command (1945-1947)	Superior War School, Paris (1924-1926)
Averescu Alexandru	Marshal (1930)	Chief of the General Staff (1911-1913); 2nd Army Commander (1916-1918)	Superior War School, Torino (1884-1886)
Bungescu Ioan	Brigadier General	Chief of Staff, 2nd Army Corps (1944-1946)	Superior War School, Paris (1932-1933)
Butoi Iosif	Lieutenant General	Commandant of the Military Academy (1949-1950) and of the Technical Military Academy (1951-1957)	Superior War School, Paris (1931-1933)
Cristescu Constantin	Army Corps General	Chief of the Great General Staff (01.04-28.10.1918; 1.04.1920-8.05.1923)	Superior War School, Paris (1892-1894)
Dragomir Nicolae	Brigadier General (1944)	Chief of Staff, the 4th Army (1944-1945)	Superior War School, Torino (1924)
Dumitrescu Polihron	Divisional General	Commander of the 21st Infantry Division (1945)	Superior War School, Paris (1921-1923)
Frunză Petre	Divisional General	Divisional Commander (1916)	Superior War School, Brussels (1881-1882)
Iarca Alexandru	Divisional General (1911)	Commander of the 3rd Army Corps (1913)	Superior War School, Brussels (1882-1884)
Jitianu Ion	Divisional General	Commander of the 2nd Army Corps Territorial Command (1928)	Superior War School, Brussels (1896-1898)
Mavrocordat Leon	Divisional General (1918)	Chief of the Royal Military Staff, Commandant of the Superior War School (1899-1900)	Superior War School, Paris (1887-1889)

Name and surname	Highest rank	Highest position	Educational institution (period; country)
Petala Nicolae	Divisional General (1918)	Army Inspector General (1920-1926)	Superior War School, Torino (1892-1894)
Potopeanu Gheorghe	Divisional General (1942)	Commander of the 7th Corps of the Army (1944)	Superior War School, Paris (1919-1921)
Prezan Constantin	Marshal (1930)	Chief of the Great General Staff (1916-1918; 1918-1920)	Complementary Staff Course, France (1883-1886)
Rozin Gheorghe	Army Corps General (1944)	Commander of the 4th Corps of the Army (1943-1944)	War Academy of Berlin (1914, one year)
Sahini Alexandru	Squadron General (1944)	Commander of the 3rd Air Region (1945)	War School in Aeronautics, Italy (1938-1938)
Schina Mihail	Divisional General	Commander of the 1st Cavalry Division (1917-1918)	Superior War School, Torino (1898-1900)
Stonescu Nicolae	Divisional General	Commander of the 4th Corps of the Army (1944-1945); Minister of Finance (1941-1942)	Superior War School, Paris (1920-1922)
Sturdza Alexandru	Colonel	Commander of the 7th Brigade Artillery (1916-1917)	War Academy of Berlin (1894-1898)
Şelescu Valeriu	Brigadier General (1946)	Commander of Anti-Aircraft Division (1947)	Superior War School, Paris (1925-1927)

English version by
Diana Cristiana LUPU

ENHANCING INTEROPERABILITY – THE FOUNDATION FOR EFFECTIVE NATO OPERATIONS –

Dr James DERLETH

The need for enhancing interoperability as the foundation for effective NATO operations is discussed by the author. In this context, it is shown that, since the end of the Cold War, interoperability has been at the heart of a debate over the viability and relevance of the Alliance in a new security environment. The shift of focus from territorial defence to multinational expeditionary missions and the challenges encountered executing them have demonstrated the limits of Allied interoperability. Moreover, interoperability challenges are considered. Some of them such as sovereignty concerns, differing national interests, cuts in defence spending, support for local defence industries, and disparities in technological capabilities can only be resolved by politicians at strategic level. In order to mitigate tactical challenges, including technological disparities, command and control, doctrinal differences, and resource gaps, NATO enacted the "Connected Forces Initiative" (CFI).

***Keywords**: interoperability; STANAG; Connected Forces Initiative; Combined Training Initiative*

> *"Interoperability is essential to ensure of NATO's forces effectiveness".*
>
> Supreme Allied Commander Transformation,
> General Jean-Paul Paloméros,
> 25 Sept. 2013

Since the end of the Cold War, interoperability has been at the heart of a debate over the viability and relevance of the NATO Alliance in a new security environment. The shift of focus from territorial defense to multinational expeditionary missions (Afghanistan, Kosovo, Libya) and the challenges encountered executing them has demonstrated the limits of Allied interoperability. While some interoperability challenges (sovereignty concerns, differing national interests, cuts in defense spending, support for local defense industries, and disparities in technological capabilities) can only be resolved by politicians at the strategic level, there are also numerous tactical challenges to interoperability. They include technological disparities, command and control, doctrinal differences, and resource gaps. To mitigate them, NATO enacted the "Connected Forces Initiative" (CFI).

The article was originally featured in *NATO Review*, 16.06.2015, see http://www.nato.int/docu/review/2015/Also-in-2015/enhancing-interoperability-the-foundation-for-effective-nato-operations/EN/index.htm

Dr James Derleth – Senior Interagency Training Advisor, Joint Multinational Readiness Center, Hohenfels, Germany.

NATO ISAF troops on Marawara bridge, October 2009, Afghanistan. © NATO

The goal of the CFI is to increase readiness and combat effectiveness by improving interoperability through expanded education and training, increased exercises, and better use of technology. To support the CFI, the Joint Multinational Training Command (JMTC) in Grafenwoehr, Germany, launched the "Combined Training Initiative" (CTI). Drawing on the JMTC's unique location and experience educating and training NATO allies and multinational partners, the CTI expands education and training and uses technology to execute integrated, simultaneous, live, virtual, and constructive exercises. The CTI greatly reduces the cost of training, fosters multinational partnerships, and most importantly, improves Alliance interoperability.

The need

> Recognizing this situation, Alliance leaders created the Connected Forces Initiative (CFI).

NATO defines interoperability "as the ability to operate in synergy in the execution of assigned tasks". Even after many years of emphasizing interoperability and NATO Standard Agreements (STANAG) to foster it, recent missions have shown the limits of interoperability. Recognizing this situation, Alliance leaders created the Connected Forces Initiative (CFI). Its purpose is to ensure NATO formations can communicate, train, and operate together effectively. Although the need is clear, there are many challenges to implementing the CFI.

The next section examines some of the main ones and how the Joint Multinational Training Command has mitigated them.

Challenges

While there are strategic and tactical challenges to interoperability, this paper focuses on the latter. This is because overcoming strategic challenges requires political decisions while overcoming them at the tactical level can be accomplished through the establishment of common tactics, techniques, and procedures (TTPs). Key tactical interoperability challenges include technological disparities, command and control, doctrinal differences, and resource gaps.

1. Technology disparities

There are vast technological disparities between NATO forces. On one end of the spectrum is the United States with its reliance on digital technology. Unmanned Aerial Systems (UAS), Command Post of the Future (CPOF), and Blue Force Tracker (BFT) are all readily available to an American commander and help him/her establish a common operational picture. However, this operational picture is not "common" if other members of a Joint Task Force can't see it. There are at least 13 different systems for battle tracking within NATO. Many of them, because of different technical standards, are not interoperable.

"To mitigate this situation, the JMTC has pursued low tech solutions".

Shadow Unmanned Aerial System (UAS) inbound! The Shadow is a tactical Unmanned Aerial System (UAS) weighing about 400 lbs. with optical and infrared cameras effective over several miles. Pictured here, a Georgia Guard platoon brings in a system for landing. © Georgia National Guard

To mitigate this situation, the JMTC has pursued low tech solutions. These include vehicle markings to identify friendly forces, using simple graphic control systems to control movement, reliance on FM radio communication, conducting rehearsals to achieve a shared understanding, and most effectively, ensuring every battalion or higher level formation has liaison officers (LNOs) to synchronize its operations with adjacent and higher level formations.

Exchanging LNOs is particularity effective as they facilitate integration and foster peer-to-peer contacts. This has both operational and long-term benefits. As MG Walter Piatt, the Deputy Commander of the US Army Europe noted: “countries don’t have relationships, people do. We gain credibility through shared hardship”.

2. Mission command and control

The past decade of war has reinforced the importance of integrated Command and Control. Operations have become very complex, distinguished by continuous interactions between friendly forces, enemy forces, and local populations. Simply giving national formations a “task and purpose” within a Joint Task Force is not enough. It requires collaborative planning and integration to develop and maintain a common understanding of the operational environment and the mission. Too often, units are deployed without knowledge of their allies’ systems or an understanding of what type of information is sent over to them. This lack of interoperability makes it difficult for units to communicate and maneuver effectively.

Dr James Derleth teaching a class

The JMTC mitigates this challenge by having its Observer, Coach and Trainer (OCT) Teams work with exercise participants before they arrive at the training center. The goal is to ensure all formations understand–and are able to integrate, each other's unique capability and capacities. This includes having each participating country identify what types of equipment they use, how many networks they typically operate, and the type of information passed over them. This information leads to a construction of a compatibility matrix which shows what systems are able to communicate over different frequencies or networks.

3. Doctrinal differences

It's not surprising that within a group of 28 countries there are significant doctrinal differences. For example in US doctrine, "Fires" means "integrating and delivering lethal and non-lethal fires to enable joint and maneuver commanders to dominate their operational environment". In contrast, NATO countries trained with Soviet doctrine employ Fires primarily in an area/barrage role. Also in contrast to US doctrine, these countries establish a "Hide" (a location approximately one kilometer from their designated Firing Point) to protect their artillery assets. This means Fires are not available for 15-25 minutes once they are called. Since US artillery assets are able to provide support in 3-5 minutes, this has a significant effect on interoperability.

Sgt. 1st. Class Anthony Craft of U.S. Army Europe's Joint Multinational Readiness Center briefs Bulgarian soldiers on tactical movement procedures during a military advisory team training exercise at the JMRC in Hohenfels, Germany, Dec. 2. The MAT and police advisory team training programs are designed to replicate the Afghanistan operational environment while preparing teams for counterinsurgency and improvised explosive device operations and the ability to train, advise and enable Afghan security and police forces. Photo by Spc. Jordan Fuller

To diminish doctrinal differences between countries, the JMTC has learned to make diversity a virtue. It doesn't force Allies or multinational partners to use US Doctrine; instead it fosters functional interoperability. As an illustration, during a 2014 exercise, the 173 IBCT(A) had a Czech 152mm artillery battery attached to it. In accordance with Czech doctrine, the battery employed concealment and movement. This caused a lag between the call for fires and their delivery. To account for this difference, the 173 IBCT (A) established event based time triggers. Once the triggers were included in the planning process, the BCT was able to successfully execute timely and accurate joint fires. Noteworthy, because of the Czech emphasis on concealment, the BCT's artillery assets were much less vulnerable to enemy attacks. This emphasis on functional interoperability improves Alliance capability and capacity.

4. Resource gaps

Sustaining multinational forces is a significant interoperability challenge. While a NATO Standard Agreement (STANAG) defines logistics as the planning and implementing force movement and maintenance; implementation of this standard varies. As in other areas, interoperability is affected by different terminology,

Czech Republic Army soldiers from 1st and 2nd Platoon Field Artillery maneuver a self-propelled gun-howitzer vehicle, called a DANA 152mm, into firing position while conducting simulated fire training during Combined Resolve at the Hohenfels training area at Hohenfels, Germany, Nov. 15, 2013. The exercise trains U.S. Soldiers, and multi-national brigades to defeat complex threats during coalition missions. Since the Joint Multinational Training Command's Grafenwoehr and Hohenfels training areas are centrally located in Europe, U.S. forces, Army, Air Force, Navy, and Marine develop unique bonds with NATO, allied and multinational forces of 38 European nations. © U.S. Army photo by Spc. Derek Hamilton/Released

parts are carried to the type of rations soldiers eat. While many countries were able to access the US supply system in Afghanistan, expeditionary deployments to the JMTC have shown that some Alliance members have difficulty providing their own ammunition, food, and fuel; let alone taking care of sanitary needs, housing, water, etc.

To foster interoperability, the JMTC attempts to implement the NATO principle of providing logistical support on a functional, rather than a national basis. Tactically, this can be accomplished through early pre-mission planning discussions between logisticians in a multinational working group. This group identifies capabilities and requirements to mitigate possible sustainment shortfalls. For example in a recent exercise, this working group identified a bulk water shortfall across the Joint Task Force. This challenge was solved by distributing water equally across the formation to ensure operations would continue unimpeded.

Although the interoperability challenges are significant, as a result of its location in the center of Europe, its unique capabilities, and its extensive experience working with Allied and multinational partner military forces over the last decade, the JMTC has been able to reduce them and provide effective, integrated training. However, it is still not at the level envisioned in NATO's Connected Forces Initiative. To implement this guidance, the JMTC launched the Combined Training Initiative.

The Combined Training Initiative (CTI)

The CTI takes advantage of changing conditions to take NATO interoperability and operational readiness to a higher level. It is based on NATO's three components of interoperability: technical, procedural, and human.

Technology

While joint planning and execution of exercises has been common throughout NATO for years, the JMTC has significantly improved interoperability through enhanced technology. For example, the JMTC's Joint Multinational Simulations Center (JMSC – located at Grafenwoehr, Germany) establishes a Joint Operations Center to control and "fight" a distributed portion of exercise while the JMRC executes the live portion of the exercise. In Exercise Saber Junction 13, the 2nd Stryker Cavalry Regiment conducted live training at the Joint Multinational Readiness Center while the Italian Folgore Brigade virtually supported its flank from Italy.

Noteworthy, both live and virtual units can be connected "up" to a NATO Corps Headquarters (the JMTC and the Allied Rapid Reaction Corps were connected for the first time in a Fall 2014 exercise); and "down" to subordinate brigades, battalions, and companies in Hohenfels and at Allied and partner training centers throughout Europe.

Noteworthy, both live and virtual units can be connected "up" to a NATO Corps Headquarters (the JMTC and the Allied Rapid Reaction Corps were connected for the first time in a Fall 2014 exercise); and "down" to subordinate brigades, battalions, and companies in Hohenfels and at Allied and partner training centers throughout Europe. The JMTC's Combined Training Initiative fosters interoperability by integrating NATO and partner assets, capabilities, relationships, and technology to create live, virtual, and constructive exercises which simultaneously connect formations from the tactical to corps level across the continent. The CTI is the first time the JMTC – or any other combat training center, has executed exercises of this complexity and scale. This program allows Allies and multinational partners to train together while remaining in their home-station locations. This reduces costs while facilitating interoperability. As an illustration, exercise Swift Response II (August 2015), will be executed simultaneously at three different training centers in Bulgaria, Germany, and Romania.

Procedural

This category fosters interoperability through doctrinal and organizational changes. The Joint Multinational Readiness Center (a component of the JMTC – located at Hohenfels, Germany) is contributing to NATO Doctrine and developing STANAGs based on lessons learned at the Center. In addition, the JMRC is identifying and codifying tactics, techniques, and procedures (TTPs) which mitigate doctrinal diversity by focusing on functional interoperability. These TTPs are disseminated via the NATO Centers of Excellence (COE) and training facilities throughout Europe and North America.

Human

This group includes education, training, and the adoption of common terminology. Seeing rotational units struggle with interoperability challenges, the JMTC initiated the Joint Common Academic Program (JCAP). It has two components. The first is the deployment of mobile training teams (MTTs) to Allies and multinational partners to conduct leader training programs, provide specialty training, facilitate the development of local training centers, and participate in military-to-military cooperation events. Not only has this been a cost effective way to facilitate standardized education and training, but these missions also mean that when NATO formations train together, they start at a higher level of interoperability and readiness.

The second JCAP component is a series of instruction modules which are given to the staffs of all members of the Joint Task Force prior to an exercise.

Soldiers from the 2nd Battalion Royal Gurkha Rifles taking part in Saber Strike in Latvia. © NATO

The seminars cover mission command, movement and maneuver, protection, logistics, fires, engagement, and intelligence; i.e. the key areas most affected by limited interoperability. During these seminars, leaders from the JMRC introduce key topics and identify challenges faced by previous units. The Joint Task Force then works with its subordinate formations to identify ways to mitigate the interoperability challenges.

Conclusion

As former U.S. Secretary of Defense Chuck Hagel noted “the most persistent and pressing security challenges to Europe and the United States are global.” Therefore we must “develop strategies to address global threats as we build more joint capacity with European militaries”. Because of its capabilities, location, and extensive experience working with NATO and partner countries, the JMTC is uniquely positioned to implement NATO training guidance. Its Combined Training Initiative improves NATO interoperability and readiness through expanded education and training and technology. This allows NATO members to work more effectively together and fosters European security by helping protect Alliance members, deterring conflict, and increasing global stability.

Statement by NATO Defence Ministers

1. We, the Allied Defence Ministers, met yesterday and today, halfway between the NATO Summits in Wales in 2014 and Warsaw in 2016, to review the implementation of key decisions taken in Wales and to direct further work. We noted the significant progress we have achieved, in particular in implementing the Readiness Action Plan.

2. We discussed the current security environment. Russia is challenging Euro-Atlantic security through military action, coercion and intimidation of its neighbours. We continue to be concerned about Russia's aggressive actions which we discussed also in a meeting with our Ukrainian colleague, Minister Poltorak, where we reaffirmed our strong commitment to an independent, peaceful and prosperous Ukraine and our firm support to its territorial integrity within its internationally recognised borders. We are also concerned about the growing regional instability to our South caused by a combination of diverse challenges and threats, including the threat posed by ISIL/DAESH. To address all these challenges to the East and to the South, NATO continues to provide a 360 degree approach to deter threats and, if necessary, defend Allies against any adversary.

3. The Assurance Measures initiated in May last year continue to demonstrate NATO's collective solidarity and resolve. As part of the Readiness Action Plan, all Allies have contributed to this significant effort in the East of the Alliance on the ground, at sea and in the air, 28 for 28. We also discussed Adaptation Measures. Defensive in nature, they ensure that NATO has the right forces in the right place at the right time, and that NATO remains a ready, robust and responsive Alliance, capable of meeting current and future challenges from wherever they arise. We are working to ensure that our forces are fully trained, equipped and maintained at the high levels of readiness, coherence and flexibility needed to conduct NATO's full range of missions, including deterring aggression against Allies and demonstrating preparedness to defend NATO territory.

4. Work on an enhanced NATO Response Force (NRF) has progressed substantially. The future NRF will be significantly larger and more capable. It will be on a higher level of readiness, more responsive and more interoperable. The interim Very High Readiness Joint

Document originally featured at http://www.nato.int/cps/en/natohq/news_121133.htm

Task Force (VJTF), led by Germany, the Netherlands and Norway, with other Allies participating, is now operational. NATO is engaged in a series of important exercises in the East of the Alliance, and we have noted with satisfaction the successful deployment Exercise NOBLE JUMP conducted by the interim VJTF in Poland last week.

5. From 2016, the VJTF brigade, led by Spain, with other Allies participating, will be available to respond rapidly to any contingency. This autumn, as part of its training and preparation, it will participate in NATO's high-visibility Exercise TRIDENT JUNCTURE 2015 which will be conducted with over 30.000 troops mainly in Italy, Portugal and Spain. We welcome the declaration by Turkey to assume the role of framework nation for a future rotation of the VJTF, in addition to France, Germany, Italy, Poland, Spain, and the United Kingdom.

6. The establishment of the first six multinational command and control elements – the NATO Force Integration Units (NFIU) – on the territories of Bulgaria, Estonia, Latvia, Lithuania, Poland and Romania, is well under way. They will facilitate the rapid deployment of Allied forces to the region as required; support collective defence planning; and assist the coordination of multinational training and exercises. Taking into account military advice on the establishment of additional NFIUs which is currently being developed, we will take a decision at our meeting in October.

7. To enhance the ability to respond quickly and effectively to any contingency, we have significantly adapted our advance planning. We have also adapted our decision making procedures to enable the rapid deployment of our troops. We have set the key elements for an effective response to hybrid threats. We will seek close coordination and coherence with the European Union's efforts in this field. We have also agreed concrete steps for NATO's adaption to the growing challenges and threats emerging from the south.

8. The implementation of the Readiness Action Plan is contributing significantly to a substantial, far-reaching adaptation of NATO's military strategic posture required to respond to the changed security situation. We have issued new Political Guidance to our defence planners to maintain our ability to fulfil all three core tasks of the Alliance, with a renewed emphasis on deterrence and collective defence capabilities, and to maintain our ability to effectively deal with any future challenges.

9. We acknowledge that transformation of our forces and capabilities and the way we employ them require sufficient funding by all Allies. We reaffirm the importance of the Defence Investment Pledge adopted at the Wales Summit. Accordingly, we are working on reversing the trend of declining funding for defence, and we will make the most effective use of our defence budgets.

10. Our discussions have encompassed all of the important defence-related work that will form part of the substance of the NATO Summit in Warsaw next year, including elements of a comprehensive long-term adaptation of NATO. The progress made today shows that NATO has increased its readiness and responsiveness to all potential threats to the Alliance, and to any contingency that might arise.

The editorial and layout process
was completed on 16 July 2015.

Cover 1: *Special Operations Forces – in action, 14 October 2014. Photo: Cristian Vlăsceanu, the Navy Media Group.*
Cover 3: *Visit at the NATO Force Integration Unit (NFIU), București, 2 July 2015. Photo: Eugen Mihai.*
See http://www.mapn.ro/fotodb/20150702_1/9W2A4467
Cover 4: *Multinational Exercise ROUSOFEX 15, Capu Midia shooting range, June 2015.*
Photo: Corporal Nicușor Comănescu.

http://www.smg.mapn.ro/gmr