



4 October
December
2010

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, 6th year -**

Romanian Military Thinking



PUBLISHER

ROMANIAN ARMED FORCES
GENERAL STAFF

EDITORIAL BOARD

CHAIRMAN

Maj Gen Nicolae TABARCIA

MEMBERS

Academician Dan BERINDEI
Lt Gen Professor Dr Teodor FRUNZETI
Lt Gen Dr Dan GHICA-RADU
Lt Gen Dr Ion-Aurel STANCIU
VAdm Dr Aurel POPA
Maj Gen Alexandru RUS
Maj Gen Dr Virgil BĂLĂCEANU
Maj Gen Dr Mihai CHIRIȚĂ
Col Dr Mircea TĂNASE

SCIENTIFIC REVIEWERS

Gen (r.) Professor Dr Mihail ORZEȚĂ
AF Gen Professor Dr Florian RĂPAN
Brig Gen (r.) Professor Dr Costică ȚENU

EDITORIAL STAFF

Editor-in-Chief

Col Dr Mircea TĂNASE
e-mail – mirceatanase2003@yahoo.com

Deputy Editor-in-Chief

Alina PAPOI
e-mail – alinagmr@yahoo.com

Editors

Iulia NĂSTASIE
Diana Cristiana LUPU
Adelaida-Mihaela RADU (Layout)

EDITORIAL STAFF ADDRESS

13-15 Izvor Street, Sector 5, Bucharest
Telephone: +4021.410.40.40/1001731; 1001732
Tel/Fax: +4021.319.56.63
<http://www.defense.ro/gmr>

Romanian Military Thinking Journal
is issued in March, June, September, December.

ISSN 1841-4451 ~ Print
ISSN 1842-824X ~ Online

COPYRIGHT: articles may be reproduced free of any charge,
on condition that appropriate credit is given by making mention
of the number and date issue of the journal

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 Bucharest on 8 December 1897

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.

4 October
December
2010

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, 6th year -

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

*Romanian Military Thinking Journal
is recognised
by the National University Research Council
and included in the "B" category*



Contents

Editorial

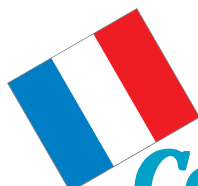
Security through Cooperation
Colonel Dr Mircea TĂNASE

Conceptual Projections

Continuous Warfare
– Confrontation Environment (II)
General (r.) Dr Mihail ORZEAȚĂ

NATO Logistic Support Concept
in Crisis Response Operations
Colonel Călin ALMĂȘAN

Transformation of Military
Organisations. Particularities
of the Romanian Armed Forces
Transformation in the Context
of the European and Euro-Atlantic
Integration (II)
Colonel Gheorghe DIMA



Contenu

Editorial

7 Sécurité par coopération
Colonel dr. Mircea TĂNASE

Projections conceptuelles

11 La guerre continue
– le milieu de confrontation (II)
General (ret.) dr. Mihail ORZEAȚĂ

29 La conception d'un soutien logistique
de l'OTAN dans les opérations
de réponse aux crises
Colonel Călin ALMĂȘAN

33 La transformation des organisations
militaires – particularités
de la transformation
de l'Armée Roumaine
dans le contexte de son intégration
européenne et euro-atlantique (II)
Colonel Gheorghe DIMA

Neopolitics • Neostrategy
International Security

Néopolitique • Néostratégie
Sécurité internationale

The Jihad and the Dynamics
of Global Security

Colonel (r.) Eugen LUNGU

43 Le Jihad et la dynamique
de la sécurité mondiale

Colonel (ret.) Eugen LUNGU

The Maritime Dimension
of Combating Piracy off Somali Coast

Lieutenant Commander

Laurențiu MEȘTERCA

57 Combattre la piraterie
au large de côtes somaliennes

– la dimension maritime

Lieutenant-commander

Laurențiu MEȘTERCA

Security Challenges *via* the Internet

Dr Petre DUȚU

77 Provocations de sécurité *via* l'Internet

Dr. Petre DUȚU

Opinions

Opinions

Tendencies in the Evolution
of Logistic Support in Future Conflicts

Colonel BEng Teodor INCICAȘ

86 Tendances dans l'évolution du soutien
logistique dans les conflits de la future

Colonel eng. Teodor INCICAȘ

Some Opinions
on a Possible Integrated
Information Management System
regarding Communications
and Information Training (II)

Colonel Dr Gheorghe DINCĂ

92 Certaines opinions à l'égard
d'un possible système intégré
de management de renseignements
qui se réfèrent à l'instruction
dans le domaine des communications
et de l'informatique (II)

Colonel dr. Gheorghe DINCĂ

Economic and Social Threats
to International Security
Dr Irina CUCU

102 Les défis économiques
et sociaux de la sécurité internationale
Dr. Irina CUCU

*International
Connections*

*Connections
internationales*

Cyber War and Cyber Power.
Issues for NATO Doctrine
Dr Jeffrey HUNKER

110 La guerre cybernétique
et la pouvoir cybernétique.
Problèmes de la doctrine de l'OTAN
Dr. Jeffrey HUNKER

Multi-Resolution Federations
in Support of Operational
and Higher Level Combined/
Joint Computer Assisted Exercises
Dr Erdal CAYIRCI

131 Les fédérations multi résolution
dans l'appui des opérations assistant
par l'ordinateur
du niveau opérationnel et supérieur
Dr. Erdal CAYIRCI

European Think Tanks: Regional
and Trans-Atlantic Trends (IV)
– report of The Think Tanks
and Civil Societies Program 2009

147 European Think Tanks: Regional
and Trans-Atlantic Trends (IV)
– report of The Think Tanks
and Civil Societies Program 2009

*Pages of Military
History*

*Pages de l'histoire
militaire*

Milestones in the History
of the Romanian Naval Forces
Commander
Dr Olimpiu Manuel GLODARENCO
Dr Florin STAN

169 Repérés historiques
des Forces Navales Roumaines
Lieutenant-colonel
dr. Olimpiu Manuel GLODARENCO
Dr. Florin STAN

<i>Military Journalistic Universe</i>	182	<i>Univers journalistique militaire</i>
<i>Editorial Events</i>	186	<i>Événements éditoriaux</i>
<i>The “GMR” Journal Awards</i>	190	<i>Les Prix de la revue “GMR”</i>
<i>RMT Mail</i>	195	<i>Correspondance RMT</i>
<i>Abstracts</i>	197	<i>Résumés</i>



Security through Cooperation

“We, the Heads of State and Government of the NATO nations, are determined that NATO will continue to play its unique and essential role in ensuring our common defence and security. This Strategic Concept will guide the next phase in NATO’s evolution, so that it continues to be effective in a changing world, against new threats, with new capabilities and new partners”¹.

Through the new Strategic Concept, adopted at the recent Lisbon Summit, NATO reasserts the Western world cohesion and solidarity regarding the Alliance’s roadmap to efficiently meet the challenges of the 21st century, by virtue of its commitment to confirm that it is a pillar of global security and, naturally, to honour the title of the most successful alliance in history.

Seeking to maintain the current consolidated power and to tailor NATO capabilities to the actual contemporary security environment, as well as to anticipate, with maximum responsibilities, the solutions meant to respond to the challenges of the future, which is many times unpredictable, the new Strategic Concept will certainly revitalise the North Atlantic Alliance.

Collective defence, crisis management and cooperative security are the three core tasks NATO is committed to by adopting this programmatic document. Concerned to strike a judicious balance between deterrence, missile defence and conventional forces, the Alliance has decided to materialise its own missile defence capability to protect all the states in Europe, asserting, at the same time, that it will consider its interconnection with the other defensive systems in the region.

Therefore, the Alliance periodically redefines its courses of action in compliance with current realities and its aspirations. It is because, as the US President states, *“each time NATO has risen to the occasion and adapted to meet the challenges of that time. [...] We now have a clear plan to protect all of our allies in Europe as well as the United States”².*

¹ *“Strategic Concept for the Defence and Security of The Members of the North Atlantic Treaty Organisation”*, adopted at the Lisbon Summit, 19-20 November 2010, see <http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf>.

² *Press Conference of President Obama after NATO Summit in Lisbon*, see <http://www.whitehouse.gov/the-press-office/2010/11/20/press-conference-president-after-nato-summit>

The Alliance consolidates and reasserts the partnership with the European Union, another institution that may have its say in security matters, and, at the same time, it declares for the open door policy and commits to developing new capabilities and new partnerships. The interest in relaunching the relations with the Russian Federation favours the option of managing globalisation in partnership, disfavouring an adversarial relationship, so we can anticipate that these relations will result in the establishment of a common security space.

The new Strategic Concept stresses the strategic importance of the Wider Black Sea Region, not only for NATO but especially for Romania, one of the main actors in this geopolitical area. The redefinition of the missions of this pillar of stability and security that is the North Atlantic Alliance provides us with a sense of belonging to a great and powerful family that strives to protect all its members. That is why we can be optimistic in this respect.

The world is changing and it is more and more difficult to understand it, as there are unpredictable mutations and not exactly encouraging prospects. History is being written before our eyes. The Lisbon NATO Summit, which is certainly one of the major events in the first decade of the 21st century, as well as the new Strategic Concept adopted on this occasion will generate multiple theoretical approaches, and our journal, a forum for debate and confrontation on the front of the genuine military theory and science, will host in its pages pertinent points of view, convinced that all combatants are winners in the battle of ideas.

In December, I think it is worthwhile to try to look forward to the coming year with optimism, hoping that a part of our aspirations, which have been more and more modest lately, will come true.

We warmly wish all the best to all those who serve the country with faith and devotion to preserve its peace and security !

Happy New Year !

 *Colonel Dr Mircea TĂNASE*

*English version by
Diana Cristiana LUPU*

Sécurité par coopération

“Nous, chefs d’État et de gouvernement des pays de l’Alliance, sommes déterminés à ce que l’OTAN continue de jouer son rôle unique et essentiel, qui est de garantir notre défense et notre sécurité communes. Le présent concept stratégique guidera la prochaine phase de l’évolution de l’OTAN, afin qu’elle continue d’être efficace dans un monde changeant, face à de nouvelles menaces, forte de capacités nouvelles et de partenaires nouveaux”¹.

Grâce à son nouveau Concept stratégique adopté lors du récent Sommet de Lisbonne, l’OTAN a réaffirmé sa cohésion et la solidarité du monde occidental sur la feuille de route par l’Alliance à répondre efficacement aux défis du XXI^e siècle, en vertu de l’obligation de confirmer son statut de pilier de la sécurité mondiale et, bien sûr, pour approprier le titre d’avoir le mieux réussi au monde.

Proposer à la fois de maintenir l’actuel pouvoir consolidé et l’adaptation des capacités d’OTAN sur le concret d’environnement de sécurité contemporain, mais aussi d’anticiper, avec la plus grande responsabilité, des solutions pour répondre aux défis de l’avenir qui est souvent imprévisible, c’est le nouveau Concept stratégique qui va certainement revitaliser l’Alliance de l’Atlantique Nord.

La défense collective, la gestion des crises et la sécurité coopérative sont les trois tâches fondamentales que l’OTAN a en assumé par ce document de politique. Soucieuse de maintenir un équilibre judicieux entre la dissuasion, la défense antimissile et les forces conventionnels, l’Alliance s’est engagée à matérialiser son propre bouclier antimissile pour protéger tous les pays européens, en exprimant spécialement qu’elle tiendra compte de son interconnexion avec d’autres systèmes de défense dans la région.

Voici, donc, une alliance qui redéfinit régulièrement son cours d’action, en ligne avec les réalités actuelles et ses aspirations. Parce que, comme il énonçait le président des États-Unis, *“à chaque fois, l’OTAN a surmonté le moment et s’adaptée*

¹ *Le Concept stratégique pour la défense et la sécurité des membres de l’Organisation du Traité de l’Atlantique Nord*, adopté par les chefs d’État et de gouvernement à Lisbonne, 19-29 novembre 2010 – *“Engagement actif, défense moderne”*, Préface, sur le site <http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf>

pour être en mesure de faire face aux défis de ce moment-là. [...] Maintenant, nous avons un plan clair pour protéger tous nos alliés en Europe ainsi que les États-Unis”².

Alliance renforce et réaffirme son partenariat avec l’Union européenne, une autre institution à travers lequel la sécurité peut être exprimée, mais en même temps la porte politique de l’OTAN est ouverte et elle s’engage à développer de nouvelles capacités et de nouveaux partenariats. L’intérêt pour la relance des rapports avec de la Fédération de Russie est en faveur de la gestion de la mondialisation dans la formule de partenariat, plutôt qu’une relation d’adversité et on peut donc prévoir l’évolution de ces relations vers un espace commun de sécurité.

Le Nouveau Concept stratégique précise aussi l’importance stratégique de la région élargie de la Mer Noire, tant pour l’OTAN, mais surtout pour la Roumanie, l’un des acteurs principaux dans ce territoire géopolitique. Redéfinir les responsabilités du ce pilier de la stabilité et de la sécurité qui est l’Alliance cela nous donne un sentiment d’appartenance à une famille nombreuse et puissante qui cherche à fournir une protection à tous ses membres. Voici, de ce point de vue, que nous pouvons être optimistes.

Le monde évolue et devient de plus en plus difficile à comprendre, avec des mutations imprévisibles et des perspectives non pas très encourageantes. Cette histoire est écrite au dessous de nos yeux. Le Sommet de l’OTAN à Lisbonne, certainement l’un des événements majeurs de cette première décennie du XXI^e siècle, et le nouveau Concept stratégique adopté à cette occasion vont générer de multiples approches théoriques, et notre revue, qui est un forum des discussions et des confrontations sur la théorie militaire et de la science authentique, sera l’hôte de points de vue pertinents dans la conviction que tous les combattants seront vainqueurs après un duel.

Maintenant, en Décembre, je pense qu’il vaut la peine d’essayer un exercice de volonté et de regarder avec optimisme pour l’année à venir, en espérant que certaines de nos aspirations, de plus en plus modestes ces dernières années, seront exaucées.

Ainsi, pour tous ceux qui servent avec foi et dévotion sous le drapeau du notre pays, pour sa paix et sa sérénité, on transmet une gentille pensée !

Bonne année !

Version française par Alina PAPOI

² La conférence de presse du président Barack Obama près le Sommet de l’OTAN à Lisbonne, sur le site <http://www.america.gov/st/texttrans-english/2010/November/20101120180210su0.4472882.html>

CONTINUOUS WARFARE

Confrontation Environment (II)

General (r.) Dr Mihail ORZEAȚĂ

The multiple dimensions of confrontation require that every decision-maker, especially the military one, should study very well the environment before any decision and action. Cyberspace, airspace and outer space make it possible for the integration of the confrontation environment to exist.

In cyberspace, there are communications and computers networks that use IT products that are sent and received through physical and electromagnetic means.

Time, opposing forces and space are the most important factors that influence military actions during war.

All the members of a coalition or an alliance have to know and obey the rules and procedures that govern them in order to win the confrontations in which they are involved.

Keywords: *confrontation; military environment; integration of the battlefield*

Under the impact of globalisation and information, the internal and international security environment is permanently changing. Some changes are unpredictable and linear, but many of them have a seismic, surprising, discontinuous or contradictory character. Although the general tendency of the security environment seems to be that of regional and then global integration, the phenomenon of state fragmentation continues to exist and even to amplify. On the other hand, the tendency to achieve an international security system is opposed to the tendency to independence of some ethnic and religious communities and some international non-governmental organisations that are willing to have a more important say (role) in the management of some domains of human activity, the security one included. These tendencies are generated by the behaviour of people who have different interests, aspirations and ideologies. In many situations, instead of having a dialogue to get to know each other better and to eliminate the differences of opinions between them through negotiation, people and communities choose to confront each other, including by using weapons.

General (r.) Dr Mihail Orzeată – Associate Professor at “Carol I” National Defence University, former Deputy Chief of the General Staff.

Under the current conditions, when “the number of the non-classical actors who have imposed their own rules in so-called private areas has significantly risen”¹ and the tendencies to erode the nation-state are more and more obvious, promoted by individuals and transnational companies², conflicts may multiply. Given the fact that most conflicts could occur within states and not between them, the characteristics of military actions and the way in which military entities carry out the assigned missions will undergo important changes.

In essence, force – perceived not long ago as being mostly destructive – will be used more moderately and carefully in order not to cause unintended, unnecessary and collateral damages. According to the UN statistics, in the conflicts occurred “in more than 30 countries, starting 1989, more than four million people have died”³, the ratio of losses being 10 civilians to a military man. Although it is estimated that conflicts physiognomy will dramatically change, we cannot exclude the classical types of conflicts and wars – state versus state and armed force versus armed force –, because they continue to exist, and the wars in Iraq, Afghanistan and Caucasus (Georgia versus South Ossetia, supported by the Russian Federation) are convincing and recent examples. Of course, there have been differences as far as approaching conflicts is concerned, influenced by the confrontation environments that have also been different.

Military actions are influenced by a multitude of factors whose effects are decisive many times. This is the reason why, before making a decision regarding the goal (objective), the way forces are deployed (procedures, the direction and area to focus the efforts, the pace at which the action is conducted, the estimated duration until the planned/desired result is achieved etc.), the adopted form of combat, decisive moments (the beginning of actions, the use of reserves etc.), a thorough analysis of the confrontation environment has to be conducted. Taking into account the fact that many of the data that have to be processed to complete the analysis are variable or estimated, the assessment of the confrontation environment has to be permanent in order to reduce the risk of surprise.

The most important factors that form the *confrontation environment* are the following: *adversary, confrontation area, climate and meteorological-hydrological situation, time, own capabilities, allies, neighbours, neutral ones, constraints and limitations.*

¹ Robert Kaplan, *Imperiul sălbăticiei: America, o națiune în comă*, Editura Antet, 2002, p. 28.

² Stephen G. Brooks, *Producing Security: Multinational Corporations, Globalization, and the Changing Calculus of Conflict*, Princeton University Press, Princeton, New Jersey, 2005, p. 5.

³ United Nations Environment Programme – UNEP, *From Conflict to Peacebuilding – The Role of Natural Resources and the Environment*, www.un.org

Adversary

It is the most dynamic factor that exercises the most important influence on the development and result of the armed confrontation. As it has happened so far and maybe it will also happen in the future, the adversary will make all the efforts, military and non-military, legal and subversive ones, to win victory.

One of the permanent preoccupations of any adversary and any military commander is the as good as possible awareness of the opponent before the beginning of and during hostilities. Data as: the organisational structure – according to hierarchical levels and types of military entities –, the deployment of the forces in the theatre of operations, the total and the services combat capability, the level of logistic support, the morale of the combat forces and the level of the population support for the military actions, strengths and weaknesses, the forces employment concept etc. are used to achieve the quantitative and qualitative ratio of forces. Based on the known data regarding the adversary, it is possible to make scenarios as far as action is concerned and to plan operations and fights.

Permanently monitoring the adversary is one of the conditions for the reduction of the probability to be surprised or misled by its actions. Moreover, having enough elements regarding the adversary, we can anticipate, prevent or successfully counter most of its actions and we may prevent it from seizing the initiative.

In order to collect, process and assess the adversary's intentions, diverse structural entities, means and methods are employed:

- the information collection by specially trained personnel – spies, scouts in the adversary disposition etc. –, constituted in HUMINT (Human Intelligence) structures;
- the observation of the electronic spectrum to detect the emissions of the electronic non-communication devices used by the adversary for: airspace surveillance (terrestrial, air and naval radars; thermo-locators; satellites etc.); aircraft and missile guidance on the trajectory; forces command (issue and transmit orders, receive reports, process and transmit data etc.); electronic reconnaissance, protection and counteraction etc., through ELINT (Electronic Intelligence) – structures properly equipped and specialised in these types of activities;
- the examination of all types of electronic signals: communications, data transmissions etc., through SIGINT (Signal Intelligence) – structures properly equipped and specialised in these types of activities.

Being aware of the importance of information in conducting military actions, the adversary will seek to conceal their actions through deceiving or masking, destroying or blocking the functioning of our assets designed to collect and process data.

Masking may be achieved through both passive methods (sheltering in spaces specially built to resist the attacks that use different combat assets, and spaces protected against the detection by all types of reconnaissance assets) and active ones (electronic simulation of the false position of some combat assets, command structures, electronic reconnaissance and counteraction assets etc.; real-scale models of some objectives and types of military assets etc.).

Deception may be achieved through a wide range of forms and methods. The most effective one is the simulation of some real activities – movement of troops and military assets to mislead the adversary over the direction (area) of effort concentration, and over the direction the attack (offensive) is launched; false radio and data traffic; engineering services in some areas that are not key ones from the operational standpoint etc. Another deceiving method that had spectacular results in past conflicts was misinformation, starting from the principle that “*A crowd may be lied easier than an individual or a group of individuals ... portioning the truth*”⁴. During the last world conflagration, the allies simulated the loss of some official documents in a plane crash. The particular documents contained the plans of disembarkation in an area other than Normandy, where it was actually planned. The documents got to the Nazis who took measures to reinforce the area in the “*captured plans*”, weakening the defence around the Omaha Beach, where the landing took place and the second front was opened on 6 June 1944.

Confrontation environment

The more and more competitive technical assets that have been produced lately and incorporated in the branch, command and control, combat support and logistic support systems have succeeded in reducing the dependence of military actions on the confrontation environment, concomitantly with its extension. However, the environment continues to influence the result of and the way any human activity is performed, armed fight included. Traditionally, the confrontation environment consists of: *the land, atmosphere, outer space, ocean and virtual environment*.

❖ *The land (terrestrial environment)*

Through the variety of landforms in the area where military actions are performed and the association with other factors – climate, hydro-meteorological,

⁴ Vladimir Volkoff, *Dezinformarea văzută din est*, Editura Pro Editură și Tipografie, București, 2007, p. 29.

light intensity etc. –, terrestrial surface determines the pace and intensity of military actions and influences their results as follows:

- reduces the possibility to discover the objectives and actions under development in hilly, mountainous and forested areas;
- hilly, mountainous and forested areas favour defence, especially in the military confrontations that make use of traditional weapons, as they offer more possibilities to mask or shelter the objectives, to dispose forces and manoeuvre, and to reduce the necessary volume of engineering services through the use of some landforms for sheltering and masking;
- hilly, mountainous and forested areas: channel the actions of terrestrial assets along the valleys and lines of communication; limit, and in some cases, make impossible the use of some types of combat and land transportation assets; diminish and sometimes annihilate radio communication that needs direct visibility between emission and reception stations;
- in association with climate and weather conditions, steep terrain reduces the pace and intensity of military actions and sometimes – or temporarily – it makes any human action impossible (e.g. heavy precipitation may generate landslides that block the lines of communication, destroy residences, electric power transmission lines, water, gas and oil pipelines etc.; steep terrain, in association with heavy precipitation and wind may partially or totally preclude the use of helicopters, paratroopers, unmanned aerial vehicles that perform reconnaissance etc.);
- desert areas are characterised by high temperatures in daytime and low temperatures at night, by low humidity, by the lack or scarcity of points of reference and lines of communication, fact that: limits the manoeuvre capacity and the pace of actions; creates difficulties related to resource supply and evacuation of assets, the wounded and refugees; offers few possibilities to mask and naturally shelter the assets, combat disposition and refugee camps; strong winds generate sand-storms that reduce visibility to zero and make impossible any human action, including the movement and manoeuvre of any type of assets;
- delta: allows for the use of heavy combat assets only in limited areas and requires for the use of amphibious assets and small and medium-seized combat river ships; abundant vegetation favours masking and reduces the pace of actions; the large number of birds and their frequent movement may limit the use of aircraft at low heights;

- polar areas: limit the use of combat and transportation assets; the lack of points of reference makes difficult the orientation through visual observation or through optical means; the areas covered with snow most of the time or the ones covered with snow permanently do not allow for masking and sheltering against attacks, especially the air ones; low temperatures require the use of special protection equipment for the personnel; because of the low temperature, the survival capability in case of accident is more reduced than in temperate, Mediterranean or tropical areas; aircraft are the highly recommended combat, transportation and rescue-evacuation assets; snow-storms may reduce visibility to zero and may make impossible the use of any type of assets and of any human activity.

❖ *Atmosphere (airspace)*

The area between the land (ocean) surface and the superior limit of the atmosphere is called *airspace*. The use of airspace for military purposes, following the invention of aircraft – balloons, gliders, airplanes, helicopters, missiles etc. –, has largely extended the confrontation environment and has significantly contributed to its integration through the use of air assets for reconnaissance, combat and transportation in common actions with the ones belonging to the land, naval and special forces. Airspace facilitates some types of military actions and limits others as follows:

- favours reconnaissance (through visual observation, photographing and electronic observation);
- contributes to the development of troops and assets transportation at distances of thousands of kilometres, at high speed, in short time, facilitating vertical manoeuvre and force protection, substantiating the concept of expeditionary force;
- favours the strike of objectives situated very far from the landing airfield and the area of direct confrontation between the land and naval forces, thus facilitating the establishment of the concepts of “*parallel war*”, “*air-land battle*”, “*in-depth strike*” etc.;
- favours command and communications across the full electromagnetic spectrum, except the situations when the electromagnetic permittivity of the atmosphere is low;
- orientation through visual observation and with the help of optical assets is difficult, at high speeds and low heights;
- favours the integration of the air-land, air-naval, air-land and naval military actions;

- the rapid development of communication assets and of the ones able to locate points of reference and objectives, the enhancement and miniaturisation of computers are elements that have contributed to the construction of some air navigation systems that allow the decrease in the dependence of air military actions on the weather conditions and the light intensity.

❖ *Outer space*

Because it is illegal to place weapons in space, space powers have opted for placing in outer space, on circumterrestrial orbits, some “platforms” – satellites, orbital stations and spacecraft – that perform missions whose results may be used in both civilian and military domain. The enormous possibilities to control any human activity carried out in the other components of the confrontation environment, through the use of space assets, determine an increase in the interests of all the communities that intend to have a more important say in the international arena, through possessing and using spatial platforms in military actions. Although there are no sufficient official data, pieces of news related to the development of devices able to guide an energy bundle towards a satellite to destroy (block) its reconnaissance, remote detection or communication devices are more and more conveyed. Space powers have also developed means and procedures to destroy the satellites of the other powers provided they become adversary, using land and naval facilities.

In order to avoid the allegations of infringement of national sovereignty of any state, the cosmic objects launched from the Earth evolve on orbits whose lower limit – perigee – is higher than the upper limit of the national airspace, as established by the space law.

Being infinite, the Cosmos theoretically allows for the extension of the confrontation environment up to this dimension. Practically, man may use only the space circumscribed by the solar system, taking into account the technical possibilities to overcome the barriers of celestial mechanics represented mainly by the speed at which vehicles may move and their capacity to overcome the gravitational pull.

The outer space favours: the reconnaissance actions through optical and electronic methods; the localisation and guidance of aircraft, vessels and combat assets towards objectives and communications by electromagnetic waves. When the transparency of the atmosphere is reduced, reconnaissance through optical means gets less accurate data. When the atmosphere is less permissive, communications and remote detection are more difficult.

The most important obstacle in using the outer space for military actions consists in the high cost and the limited access to high-performance technology.

❖ *The ocean (maritime environment)*

The ocean consists in the great mass of salt water that covers most of the Earth's surface⁵ and it is called *maritime environment*⁶ by military experts. Oceans, seas and rivers condition the development of military actions through the “*specialised platforms*” – surface ships and submarines, which may be used for fight, transportation or scientific research etc. Technical and scientific progress in the last decades has allowed for the spectacular evolution of the possibilities to use the ocean for a wide range of human activities, especially military ones. Through the construction of nuclear-powered vessels that allow navigation on and under water for many months without being refuelled, associated with the enhancement of navigation assets irrespective of time, season and weather conditions, military forces may be projected almost anytime and anywhere. To this end, aircraft carriers, helicopter carriers, landing craft (troops and assets), surface vessels and long- and medium-range ballistic missile submarine carriers are used. The association between the naval transportation platform, the air platform for the transportation of missiles, bombs, projectiles, troops, materials, ammunition, reconnaissance and electronic counteraction devices etc. represents the basis for the integration of the first three components of the confrontation environment – the land, air and naval ones.

States sovereignty over the maritime space is regulated through treaties and conventions and is symbolically represented by maps. However, these frontiers are permeable for the maritime and air platforms even in peacetime (by illegal emigrants, smugglers, poachers and other offenders – especially those whose object of activity is organised crime and terrorism). This represents a security vulnerability, in peacetime, and a defender vulnerability – at war. The physical characteristics of the maritime environment represent the favouring or disfavouring elements for any type of military action, as follows:

- lack or scarcity of points of reference – islands and cliffs at large distance – make orientation without specialised devices difficult, in any light intensity conditions;
- being an open space, it is difficult to mask or hide from reconnaissance and attacks, especially the ones executed from the air and the outer space;
- the shallow depth of waters in some areas makes navigation with large tonnage vessels impossible and requires for the use of some vessels especially designed for landing;

⁵ *Dicționarul Explicativ al Limbii Române* – DEX, Editura Academiei RSR, 1984, p. 617; *Webster's II New College Dictionary*, Houghton Mifflin Company, Boston, New York, 1995, p. 757.

⁶ *Lexicon militar*, Editura Saka, Chișinău, 1994, p. 300.

- the structure of the shores may favour disembarkation with classic landing craft on the open beaches, lagoons etc. or may make landing impossible on the high shores, shores preceded by coral reefs, and that is why air-cushion landing craft, helicopters or parachuting from airplanes or gliders should be resorted to;
- strong storms generate high waves and hinder or even prevent surface vessels from moving, so they have to wait for the reduction in the waves dimension to resume movement;
- in polar areas and in their vicinity, ice banks and icebergs float, which may cause vessels blockage, damage or even shipwreck; moreover, in these areas, water temperature is low and it is less likely for human beings to survive, in the event of an accident, without special protection equipment.

❖ *Virtual environment*

It is also called “*info-sphere*” or “*cyberspace*” and it is considered a separate dimension of the confrontation environment, although it physically overlaps with the land, atmosphere, outer space and maritime environment and it is part of any human activity, thus decisively contributing to the integration of the confrontation environment.

Communication networks and computers act in the virtual environment, using information technology products (software, protocols, databases, electronic mail etc.), which are delivered and received through physical and electromagnetic support.

The information component of modern warfare is very important for the development and result of military actions and warfare, in general, being a genuine power multiplier and “*ranked*” as “*electronic warfare*” by some American experts. Information and computer science have become sine qua non conditions for the existence of any organisation, of a modern military body included, and that is why the USA has launched the concept of “*information domination*”, which has been taken over by NATO, as part of the *Revolution in Military Affairs (RMA)* and of the continuous transformation.

Confrontation in the virtual environment is permanent, but it is especially covert and subversive, usually in association with the intelligence and psychological components. The cumulative effect of these components may decisively tip the balance of victory in favour of the party that is better prepared, more incisive, the one that better exploits opportunities and emphasises strengths rather than weaknesses. All command and execution civilian structures, in all the fields of activity, use information and have physical supports for its transmission, reception and processing. The multitude of devices that are used in common

– from the telephone, fax, radio and television sets, mobile phones to personal computers –, as well as the specialised ones – for civilian and military purposes – use virtual environment to function. As a consequence, this type of environment may be used without negatively affecting the other users or, on the contrary, it may become a theatre of confrontation.

Confrontation may occur unintentionally because of the mismanagement of frequencies, of the location of emission-reception devices at too short distances ones from the others, generating interferences or troubles as far as functioning is concerned, because of the improper isolation of the physical support for the information transfer etc. To prevent such undesirable events as well as the unauthorised access to information, experts have achieved the information protection through physical (shielding, isolation etc.) and information technology (software, passwords, encryption etc.) methods. Thus, information is available and transparent for the authorised persons and inaccessible to adversaries and intruders (hackers).

Time

Time is known to be infinite – for the Universe –, but human beings, constrained to exist for only a variable and finite period of time, under the imperative of its implacable flow to the moment of passing into non-existence, have a different perception of time. Hence the great importance attached to this dimension of the confrontation environment that stimulates some people to leave the mark of their ephemeral existence on the Earth through deeds that are not always worth praising. Time has a certain significance for any human activity, from that of being a reference element of the effectiveness assessment system (time is money) to the one of being an inseparable part of planning and coordinating processes related to all the military and civilian actions.

Military actions, maybe more than civilian activities, are influenced by the time factor, because:

- most of the military actions, especially in crisis situations and at war, are conducted using weapons and any error is translated in human life losses and important damages or environmental pollution;
- in time, cooperation, coordination and the integration of the actions of more military and civilian entities are achieved, with a view to fulfilling a common goal (e.g. aircraft taking off, attack and landing, artillery support, execution of counterattack or counter-strike, departure or arrival of the transportation means for ammunition, fuel, spare parts, food, medicines and other products necessary for the forces engaged in fights, for the wounded, refugees, disaster victims etc. may represent salvation

or, on the contrary, the loss of hope and the considerable diminution of the morale, or loss of life, defeat etc., if the particular means of transportation, combat and support do not take action timely);

- time cannot be compressed or dilated by human beings (an exception is represented by the cases when movement is performed at the speed of light or even at a speed higher than it) and that is why the absence of a rigorous time management leads to chaos, which may have negative or even catastrophic consequences; on the other hand, time management has to also take into account the flexibility of some terms that depend on many variables, among which the adversary and weather conditions, which may be at the origin of the lead or lag regarding the initial or final moment of some actions (if the attitude of the adversary is different from the estimated one, which materialises in offensive or withdrawal, then our planning should be adapted to the new situation; if meteorologists forecast a storm on the sea or land earlier than it has been estimated or if the movement of the air mass that brings storm changes direction and may affect the own forces disposition, then appropriate measures to adapt actions planning should be taken, with regard to the lead, lag, postponement or even cancellation of some actions that cannot be performed in stormy weather, such as the action of aircraft and surface vessels);
- military actions coordination according to time factor is very important but, many times, coordination has to also take into account other dimensions of the confrontation environment, especially the space factor so that the desired effect can be achieved;
- time is associated with the timeliness or the favourable conditions to perform an activity and to meet success [e. g.: 1) “*windows of opportunity*” for the launching of satellites, spaceships and spacecrafts; 2) the 1967 Arab-Israeli War, known as the Six-Day War, Israeli Air Force achieved air supremacy and decisively contributed to winning victory using a “*window of opportunity*” that consisted in launching a devastating attack on the elements of the Egyptian Air Force disposition exactly when the airspace of the country was exactly appropriate].

Even if many people consider time as an enemy, as “*its flow is always cruel*”, the military, in general, and military planners, in particular, have to be well aware of the important part it plays in our daily existence and in the situations when military entities have to act. It is true that time can be compressed or dilated only under the conditions explained by Einstein in the theory of relativity, which cannot be met for the time being by the current civilian or military assets.

However, we can free ourselves from time pressure or we can avoid, most of the time, the “*shortage of time*” on condition we are well informed, we have access to “*up-to-date*” information, we prove flexible when making plans and programmes, though firm when it comes to meeting the established goals.

Allies

A military alliance is “*an agreement sanctioned by a treaty, through which the signatory states assume the mutual obligation to act, with all or a part of their armed forces, against a common adversary*”⁷.

Alliances have to be studied in the dynamics of events so that useful conclusions can be drawn. An alliance formed in peacetime represents a key factor to discourage any potential adversary. It is important for the force of the alliance to be assessed or proved so that the particular alliance credibility level can be the one estimated at the moment the alliance is established. NATO is considered to be the most powerful political-military alliance of all times, not only due to the number of states that form it but also due to its manifestations in the political and military domain in the 61 years that have passed since it was established [e. g.: 1) the establishment of the Multinational Coalition with the majority of forces from NATO member states and the liberation of Kuwait, following the Iraqi occupation – in 1991; 2) the intervention in Yugoslavia to stop the ethnic cleansing of the Albanians in Kosovo – in 1999; 3) the overthrow of the Taliban regime and the beginning of the War on Terrorism – in 2001, in Afghanistan etc.]. Although it is not considered a political-military alliance, the European Union has also a developing military dimension that has preponderantly got manifest in humanitarian and peacekeeping missions (*Darfur*, in Africa, *EUFOR* in Bosnia-Herzegovina, *EULEX* in Kosovo etc.).

It is very important that, after the military actions are launched, alliances should keep their unity and even improve their force, through either attracting new allies or directing more resources to the economic and military domain, to enhance the military entities combat capacity. Allies exert their influence on the development and result of military actions and war, in its entirety, in many domains:

- *at political level* – through the enhancement of the ratio of forces compared to the adversary, the increase in the level of the population and troops morale – in the case of the increase in the number of the states in the alliance or through the increase in the allies efforts at economic, financial and military level to win victory – or, on the contrary, the reduction of the ratio of forces compared to the adversary, the diminution of the morale

⁷ *Ibidem*, p. 19.

of the troops and the population of the states that have remained in the alliance – in the case one or more states leave the alliance or they refuse to increase the effort at military level [e. g.: 1) during the First World War, after the Bolshevik Revolution in 1917, Lenin decided for Russia to get out of the war and to make separate peace with Germany, Romania having to fight alone, on three fronts, against the German, Austro-Hungarian and Bulgarian forces, which resulted in losing many battles and an important part of the territory, followed by making separate peace – in 1918 – with Germany; 2) the fact that the United States of America entered the war, in both world wars, caused the considerable change of the ratio of forces compared to the adversary and the victory in war of the alliances the USA was part of];

- *at economic level* – through different forms of aid for the supported party (products, services and technology supplies; long-term credits, in advantageous conditions; raw materials, materials and military assets etc. supplies) and through actions that lead to the diminution of the adversary economic capacity (counter-advertisement for the adversary products; production sabotage and access denial on some commodity markets; conditioned or even banned access of the adversaries to credits, resources, knowledge, technologies etc.);
- *at military level* – through expanding or reducing the area of confrontation with the territory of the state (states) that join or leave the alliance; some states joining or leaving the alliance may require the rethinking of some operational plans, cooperation and, sometimes, even the reevaluation or reformulation of the war goals (e. g.: through the USA, Bolivia, Brasilia, Costa Rica, China, Cuba, Ecuador, Guatemala, Honduras, Panama, Peru and Uruguay joining the Entente, in 1917, this alliance member states benefited from the modification of the ratio of forces for their advantage: 521 divisions compared to only 369 of the Central Powers and important economic and financial advantages, fact that resulted in the increase in the Entente offensive actions on the majority of fronts⁸; the war and operations goals are established through consultations between the allies, fact that usually increases the duration of the information-decision cycle; for the effectiveness enhancement and a reduced resource spending, the allied armed forces have to be interoperable; until interests are fully harmonised, frictions between the allied states and even between their military commanders etc. may occur.

⁸ *Curs de Istoria Artei Militare*, vol. II, Editura Academiei Militare, Bucureşti, 1990, p. 215.

Climate and the hydrological-meteorological conditions

Temperature and humidity extreme conditions have a rather important negative influence on military actions, through diminishing the efficiency of all categories of personnel and assets. This is the reason why, in order to reduce the influence of environmental conditions on the personnel and assets, a series of preventive measures should be taken, as follows:

- personnel should be trained and acclimatised in conditions that are almost similar to the ones in the environment where they are to conduct actions, and should be provided with the adequate protection equipment;
- assets should be protected against high temperatures, sand, dust, humidity etc.;
- resources assigned to military entities should be supplemented, above the level stipulated by norms, so that the actions could be conducted even if food, medicines, spare parts, ammunition, fuel, lubricants etc. cannot be supplied rhythmically;
- the increase in the commanders' degree of independence and competences so that they could continue the actions in the event military entities are isolated for certain periods of time because of some meteorological phenomena (snow or sand storms, monsoon rain, hurricanes etc.) or of the adversary that may block or surround military entities;
- the enhancement of the competences and equipment of the combat support and logistic entities, so that they could solve, by themselves, some problems that are usually solved by superior echelons.

Own forces capabilities

The assessment of the own forces capabilities to accomplish the assigned missions is meant to document the commander of the military entity that has been assigned the mission regarding the sufficiency of available forces and resources to meet the set goal. In order to be able to make correct decisions in any type of military action, each commander must have a picture of reality as thorough as possible, namely to know exactly: what is available to him and what he can do – in different situations – with the entity he commands; what is available to the adversary – in the case of armed fight; the time, season, weather and environmental conditions in the area where military actions are to be conducted; who are the ones he can cooperate with and what their combative capacity is; how he can be supported and in what conditions etc.

After the available data have been analysed, the commander and military planner have to compare the capacity of the own military entity to the one of the adversary – in armed fight actions –, and to the capacity he may need to accomplish another type of mission, to assess the chances of success and to demand, if needed, to tailor the structure of the organisation, procurement, available resources volume and quality to the requirements of the environment and mission.

The comparison of the combat capacities of the parties in armed fight actions leads to a result called *ratio of forces*. It is calculated, in general, and according to directions (offensive or denial – in defence) – using the equalisation procedure for the combat assets and the types of military structures –, and according to the types of major military assets.

The ratio of forces may indicate the superiority of one of the parties or the relative balance between them. In case one of the entities is superior, there are conditions for it to conduct offensive combat actions to gain initiative and to win victory in operation (fight). The party that is inferior generally adopts defence as a form of fight until it succeeds in diminishing the combat potential of the adversary to a value that allows it to take the offensive. In the situation of a relative balance, each party has to find the ways to surprise the adversary to cause as many damages as possible and to achieve superiority – in general or in some areas – to take the offensive and win victory.

Another way of achieving superiority is represented by the alliance with other states.

Domestic and international public opinion

International public opinion has been – as there are no reasons to make us think it will not be – the subject of manipulation in order to generate pressure on governments, governmental and non-governmental organisations, mass-media and all the other structures and communities that may serve the interests of those that initiate the process to influence it. An argument in this respect is offered by a former member of an intelligence structure in the USA: *“the solitary scholar who skims through piles of documents and sealed archives ..., discovers hidden words, buried under coats of fragmentary information, falsity and, in some cases, genuine disinformation; tens of years after the end of the war, the documents come to light, disclosing the hidden origins of the celebrated victories and suffered defeats”*⁹.

Some political decision-makers have not attached too much value to the force of the public opinion. However, they have been forced to incline to the will of the many

⁹ Thomas B. Allen, *Declasificat. 50 de documente strict secrete care au schimbat istoria*, Editura Curtea Veche, București, 2009, pp. 5, 9.

who vote and pay taxes ! (the US President, Richard Nixon, was dismissed from office as he decided to spy on political opponents).

In the *Cold War* and *Iron Curtain* period, each of the parties in the “*strange conflict*”, as it is called by André Fontaine in his *History of the Cold War*, struggled to point at the other with the intent to demonise it. Otherwise, the American President Ronald Reagan called the USSR the “*Evil Empire*”, and the USSR “*clients*” in the Near East called the USA the “*Great Satan*”. The most eloquent examples are the Vietnam War and the USSR interventions in Czechoslovakia and Afghanistan: while the socialist and communist states stigmatised the capitalist interventionism in Vietnam, the USA and its allies at that time took their revenge for the intervention of the Warsaw Pact – except Romania – in Czechoslovakia¹⁰, and the USSR intervention in Afghanistan respectively.

The force of the domestic and international public opinion is considerable but it gets manifest after a relatively long time interval if it is not constantly stimulated with ability. In the case of the US-led Multinational Coalition intervention in Vietnam, more than a decade was necessary for the international public opinion, and subsequently the domestic one, to determine the withdrawal of the forces without glory, fact that was considered a real defeat.

In the case of the invasion of Kuwait by the Iraqi troops in 1990, with the purpose of annexing it and transforming it in an Iraqi province, the international public opinion reacted rather quickly, stimulated by the Arab states and Western democracies that were afraid that Iraq would continue its aggressive actions in the other neighbour states. The consequence: the establishment of the Multinational Force led by the USA, which obliged the Iraqi forces to withdraw from Kuwait within less than a year.

NATO intervention in Kosovo and in Serbia, in 1999, was determined following a scenario that was similar to the one that led to the outbreak of the First Gulf War. After the confrontations between the Serbian order forces and the Albanian paramilitary forces in Kosovo, the international public opinion, especially the one in Western and Muslim countries, requested the UN Security Council to approve the military intervention to put an end to ethnic cleansing and violence. Russia's veto did not allow for the force to be authorised under the UN mandate, so NATO decided to intervene without this authorisation¹¹. The consequence: Kosovo separated from Serbia de facto and it was placed under the UN international administration,

¹⁰ Dr. Lucian Petrescu, *Patru decenii de la intervenția militară în Cehoslovacia (august 1968) a Tratatului de la Varșovia. Poziția României, consecințe și implicații pe plan internațional*, in the volume *Pagini din diplomația României*, vol. I, Editura Junimea, Iași, 2009, pp. 119-131.

¹¹ Madeleine Albright, *Doamna secretar de stat. Memorii*, Editura Rao, București, 2008, pp. 557-576.

and in 2008 it declared its independence unilaterally, which was recognised by a part of the states in the world, among which the majority of the Western states.

Before the intervention of the Multinational Coalition in Iraq, in 2003, the USA developed an ample international campaign to convince the public opinion with regard to Saddam Hussein's aggressive intentions to obtain nuclear, chemical and biological weapons. However, it did not succeed in determining all the permanent members of the Security Council to approve the military intervention: "*China, France and Russia stood firm in their decision to allow more time to the United Nations inspectors in Iraq before the military action was authorised ... [because, A. N.], the chief UN weapons inspector, Hans Blix, told the Security Council that he and his colleagues had not succeeded in discovering weapons of mass destruction in Iraq. Mohamed El Baradei, the chief of the International Atomic Energy Agency, announced the Council that the inspectors had not succeeded in discovering any proof that Iraq would have revived its nuclear programme*"¹².

Constraints and limitations

Constraints and limitations refer to the framework within the actions are developed, which conditions the way the military forces and assets are used.

Constraints consist of non-material elements and they refer to: domestic and international regulations regarding the law of peace and war, political and military objectives set for the war or conflict, the superior echelon directives, the mission assigned to the military entity that conducts the action and its commander conception regarding the accomplishment of the mission, the missions assigned to the military or civilian entities that perform actions in the same area, the details regarding the cooperation with the other neighbouring military entities, the attitude of the population in the area of operations etc.

Limitations are preponderantly physical conditions: the competitiveness of the combat technique and assets, the configuration of the physical environment where confrontation takes place, the quantity and quality of the forces and resources that are employed in the confrontation by the belligerent parties, the available time, climate, and hydrological and meteorological conditions etc.

*

The confrontation environment of today and the one estimated for the future are characterised, among others, by: the often – and many times – sudden changing situation; the rapid pace of some events; the unparalleled amplification of the number

¹² Tyler Drumheller, Elaine Monaghan, *Pe marginea prăpastiei*, Editura Minerva, București, 2008, pp. 136-137.

of factors that influence military actions; the increase in the number of direct but especially indirect “actors” that take part in the preparation and conduct of military actions; the extraordinary extension of the confrontation environment. All these characteristics do not allow for the commander to analyse the situation, to make decisions and to command his forces by himself. The time when commanders and their staff installed on a dominant landform from where they could see all the area where fights were conducted and make decisions in accordance with the evolution of the fights they monitored “live” is over ! The confrontation area has extended so much that it is impossible for a single individual to exert the integral control over the situation. The commanders of the 21st century have access to information in real or almost real time, but there are thousand of sources of information – human and electronic ones (small, medium and long range radars, hydro-locators, sonar, goniometric stations, infrared vision devices, photo and television cameras on aircraft, satellites, vessels, land combat assets etc.) –, which have to be integrated in order to have the big picture. The exponential increase in the quantity of the data that have to be analysed requires for working in a team consisting of the commander and his staff, in order to select the important data, to renounce the unimportant ones, to synthesise them and to use the synthesis to establish the courses of action and, subsequently, to make the decision and establish the details regarding its implementation.

To make a correct decision, under the circumstances in which some situation data (weather conditions, the adversary actions, and the way they change the confrontation environment, the pace of losses and the evolution of the ratio of forces between parties etc.) change permanently compared to the values considered in the preparation phase, requires the use of some methods that should forecast and describe this evolution. Based on the forecast, decisions will be made, taking into account the trends in the evolution of the confrontation environment so that decisions should not be modified in their essence, even if some of the execution details should be tailored to the concrete data of the situation during the action. In other words, in the current and predicted confrontation environment, because of the immense volume of data and the high degree of incertitude as far as their correctness is concerned, the logic and experience of a single individual are not sufficient any more.

English version by
 *Diana Cristiana LUPU*

NATO LOGISTIC SUPPORT CONCEPT IN CRISIS RESPONSE OPERATIONS

Colonel Călin ALMĂȘAN

Logistics support in NATO Crises Response Operations is grounded on the logistic potential of the participating nations, as well as on the balance between the collective responsibility and the national one. From this point of view, the implementation of multinational solutions could generate a better allocation of resources, and an increased efficiency in operational logistics.

The participation of civilian contractors has become a necessity and a responsibility, regardless of the area in which the mission may take place.

Keywords: *responsibility; logistics support; crises; multinational operations*

In conformity with the legislation in force within NATO, the member states responsibilities related to the logistic support for the forces that participate in a multinational operation are collective¹. Thus, according to the provisions of Annex A, MC 319/1, NATO commanders at agreed levels have the authority to redistribute specified logistic assets committed by nations for the support of the forces under their command.

In this respect, we would like to highlight the fact that the redistribution of the available resources is not “*a routine procedure*”², but only a “... *temporary expedient to overcome unanticipated deficiencies in support of an operational mission*”³.

In the context of the above-mentioned facts, redistribution is made to supplement the stocks of materials introduced in the theatre of operations by the structures that participate in the crisis response military action.

The responsibility for the military equipment and maintenance lies with NATO member nations. The logistic resources made available by nations represent an important component in achieving the set objectives, constituting the major part of the capabilities earmarked for NATO high commands. In this respect, the national forces are required “... *to deploy with a coherent logistic structure*

Colonel Călin Almășan – Commander of the 3rd Territorial Logistics Base.

¹ MC 319/1, *NATO Principles and Policies for Logistics*, Brussels, 2001.

² *Metodologia planificării și organizării sprijinului logistic internațional al forțelor proprii*, București, 2008, art. 7, aln. 2.

³ *NATO Logistics Handbook*, chapter 13, art. 1302, Brussels, 2001.

*tailored to their anticipated employment and nations have first call on those logistic resources*⁴. In all the cases, NATO commanders may decide how to redistribute the logistic resources (reserves) of each structure that take part in the military action, to provide solutions for certain deficiencies unanticipated during the planning process.

In accordance with NATO logistics doctrine, redistribution should not be confused with the reallocation of resources. While reallocation is usually executed only in a declared Emergency-in-War and only at the higher levels, redistribution is a logistic measure taken by the NATO commander in multinational crisis response operations to meet the needs of the subordinate echelons in order to allow them to react in real time (rapidly) depending on the changes in the operational status, during the course of military actions. Logistic resources, as it is known, cover a wide range of products and services. Logistic resources represent, in the common acceptance, the aggregate of the personnel, equipment, materials and services made available to the multinational force, namely all that act to its benefit.

Referring to the logistic personnel, it should be highlighted that it consists only in the professionals who work within established logistics structures, who will be redeployed similarly to the other units from the armed forces services. The logistic resources may be the subject of redistribution if NATO commanders consider them essential for the execution of the operational mission.

The multinational force (MF) commander does not have the necessary authority to redistribute logistic resources such as: fixed installations; complete weapon systems; civil resources, except those provided under Host Nation Support (HNS) or other agreements; personnel replacement; ensuring resources for non-NATO nations if it is not specifically approved by the providing nation.

In multinational crisis response operations, the logistic support functions are usually generated based on the collective responsibility of the Alliance member countries (the forces participating in multinational operations) in this domain and they are related to the following aspects:

- a) the logistic cooperation between NATO governing structures and nations in terms of operational requirements;
- b) the responsibility of each nation to provide its forces with the necessary equipment and logistic resources;
- c) the MF commander responsibility to establish the resources that are necessary for the own forces support and the coordination of the logistic support planning within the area of responsibility;
- d) NATO commanders' decision authority with regard to the use of the resources made available through the collective effort of the nations that participate in such a multinational operation.

⁴ *Ibidem*, chapter 13, art. 1303.

NATO forces commanders have to correctly anticipate the quantity and quality of the logistic support provided by both military and civil structures⁵.

The logistic support for the own troops engaged in crisis response operations must be provided on a continuous basis throughout the conduct of the military operation. In this respect, each nation bears full responsibility for providing the logistic support for the forces participating in NATO-led operations. There are certain exceptions represented by “... *the situations in which some NATO commanders have to negotiate and coordinate specific arrangements to ensure the force logistic support in an appropriate manner*”⁶.

NATO logistic support concept stipulates, inter alia, that between the civilian and military sectors a high level of cooperation should be established, one that has to lead to the profitable use of available resources, in accordance with the principles of logistic support in multinational operations.

In this respect, it may become a habit that, during the multinational operation, depending on the participating nations, a multinational logistic model or even a combination of models should be adopted, if the solution proposed by them meets the operational requirements. Such an option may be beneficial in providing multinational forces with the necessary logistic support, if cooperation in this domain is properly conducted. That is why, it is essential that the logistic support activities should be coordinated between NATO and national authorities, and it should be extended to all the levels of military art. This coordination must also take into account the resources of non-NATO countries, and those of the countries that are members of the UN, EU, OSCE and other bodies and organisations.

In the context of these goals, it is necessary to also establish a multinational logistic structure in the theatre of operations, one able to ensure “... *the coordination of the entire logistic support between participating nations, host nation and non-governmental organisations*”⁷ and to meet the requirements related to the coordination of available resources in the theatre of operation.

Military experts consider that the *Multinational Joint Logistics Centre – MJLC* should be regarded as an essential pillar in providing the multinational force with joint logistic support. MJLC concept describes “...*the tools in terms of structures and procedures which the NATO Commander needs to exercise his logistic authorities and responsibilities in an effective and well coordinated fashion*”⁸.

⁵ *Metodologia planificării și organizării sprijinului logistic internațional al forțelor proprii*, art. 4, aln. 1, București, 2008.

⁶ *Ibidem*, art. 5, aln. 2.

⁷ *Ibidem*, art. 4, aln. 1.

⁸ *NATO Logistics Handbook, op. cit.*, chapter. 13, art. 1312.

During the participation in military crisis response operations, the logistic support is executed in accordance with the provisions of the commander of the strategic or operational echelon who runs the operation. He establishes and enforces, together with the commanders of specialised units, the logistic support concept.

The concept is based on the logistics components and requirements, is developed following the general rules of preparation and decision-making and results from the adoption of that course of operation that best meets the commander's intention and vision.

The logistic support in crisis response operations is highly influenced by: the existing international treaties and agreements with the security organisation under whose aegis the mission/operation is conducted; the nature of missions/operations that are to be carried out; the value, organisation and equipment of the participating forces; the place and the specifics of the area in which the mission/operation is conducted; financial considerations, such as the reimbursement system established on the basis of a memorandum of understanding.

In connection with the subject matter, we wish to emphasise that the whole concept of logistic support is intended to provide support for the benefit of both national and multinational forces, taking into account not only the different specialised structures, but also the composition of the multinational force. In other words, the logistic support will be based on the national provisions in the field and may include various degrees of multinational support, as approved and accepted by the respective states. In general, while, in principle, each nation assumes responsibility for providing support to its forces, there are also other options such as the Host Nation Support, if available, the Lead Nation (LN), the Role Specialist Nation (RSN), Mutual Assistance (MA), the Multinational Integrated Logistic Units (MILUs) and/or the Multinational Integrated Medical Units (MIMUs), if this course of action is considered better.

Finally, we wish to emphasise that, in recent years it has been demonstrated that the importance and role of the logistic support have increased, according to the scope and diversity of crisis response operations; moreover, it has resulted that military structures, on their own, do not succeed in providing the participating forces with the necessary logistic support. In this regard, the participation of civilian contractors has become a necessity and a responsibility, regardless of the area in which the mission may take place. Therefore, multinational solutions as well as the use of civilian contractors are key elements in providing forces with the necessary logistic support.

English version by
 *Diana Cristiana LUPU*

TRANSFORMATION OF MILITARY ORGANISATIONS

– Particularities of the Romanian Armed Forces Transformation in the Context of the European and Euro-Atlantic Integration – (II)

Colonel Gheorghe DIMA

At the beginning of the millennium, the world entered a new phase of development marked by the coexistence and confrontation of positive trends with others that generate major risks and threats.

Under the influence of changes in the security environment, of the new forms of expression of specific risks and threats, the transformation of the Romanian Armed Forces structure is a natural process that will enable the organisation and preparation of forces for participation in national or collective defence, the improvement of the capacity for the full range of multinational crisis management operations, the fight against terrorism and the fulfilment of other tasks assigned to them.

Keywords: *Romanian Armed Forces evolution; national security; NATO/EU transformation; medium and long-term transformation*

Romania's becoming a NATO member, in 2004, and a member of the European Union, in 2007,

represent two important moments in its evolution in the 3rd millennium, as they have directly contributed to the modernisation of the Romanian society in the aggregate. NATO integration and the EU integration, two complex processes Romania performs, acting in an area of security based on common values, interests and objectives, on the principles and norms of democracy, the rule of law and market economy, provide our country with the favourable conditions for an accelerated economic and social development, the participation in the actions meant to preserve peace and security at regional and global level, the effective counter to the classic and asymmetric risks and threats.

For the Romanian Armed Forces, the period that followed the accession to the two international organisations has been characterised by profound transformations with a view to tailoring to the new realities in the Romanian society and to the regional

Colonel Gheorghe Dima – Structure and Armament Planning Directorate, the General Staff.

and global geostrategic environment. These have been the natural continuation of the ample process started in 1990 and they will be followed by new transformations, able to ensure the full integration in NATO and the EU.

As the period 1990-2010 has been thoroughly analysed by military experts, we will highlight the most important milestones that characterised the transformation of the Romanian Armed Forces up to accession to NATO, as well as the current directions of evolution. Based on these elements and the trends in evolution in the field of security that are manifest at the European and Euro-Atlantic level, we will analyse the main coordinates of the Romanian Armed Forces transformation in the medium and long term.

Milestones in the Romanian Armed Forces transformation up to NATO integration

The year 1990 represents the moment the Romanian Armed Forces entered an ample, complex, multidimensional and continuous transformation process that is aimed at the enhancement of the capability of this important institution of the state to fulfil, under any conditions, the assigned constitutional missions and the commitments assumed by our country at international level. The successful transformation has allowed for the armed forces to adapt to the changes determined by the evolution of the Romanian society in the social, economic, cultural, political and other domains, as well as to the ones in the security environment in the area, region or the world.

The major transformations of the Romanian military body in the period between 1990 and 2004 were strongly influenced by the evolution of the domestic and international situation¹.

Domestically, the situation of Romania in the period that immediately followed the year 1990 was characterised by the political and social unrest, caused by the “*birth*” of a new society. *Externally*, the main elements that may characterise the evolution of the situation were: the dissolution of the Warsaw Pact, the end of the *Cold War*, the outbreak of conflicts in the Balkans, the worsening of the already existing conflicts in other parts of the world, the terrorist attack on 11 September 2001².

What characterised the evolution of the Romanian Armed Forces in that period was their transformation from a mass, oversized army, organised to meet

¹ General-maior dr. Mihail Orzeată, colonel dr. Costinel Petrache, *Reforma armatei în perioada 1990-2004*, in ***, *Statul Major General, 1859-2004, Istorie și transformare*, coordinator general-maior dr. Mihail Orzeată, Centrul Tehnic-Editorial al Armatei, București, 2004, p. 274

² *Ibidem*, p. 276.

the requirements of the *Cold War* into a modern army, properly organised, trained and equipped, able to carry out, in the new security environment, the missions set by the Constitution: *to guarantee the state sovereignty, independence and unity, territorial integrity and constitutional democracy.*

The initiation and subsequent intensification of the relations with NATO (at the level of officials, joint activities with NATO member states and the PfP partner states) led to a better knowledge of the Alliance and its requirements for the states aspiring to integration. This resulted in a new approach to transformation, in relation to programmatic documents such as: *Romania's National Security Strategy, Romania's Military Strategy, the Government White Paper*, which covered the period's primary objective – NATO integration. Complex concepts were developed, which governed the transformation of the military field as a whole: *"FARO 2005-2010", "Project Force – 2005", "Objective Force 2007", "Objective Force – fundamentally reviewed", "Romanian Armed Forces Transformation Strategy".*

Evolutionary trends in the field of the Armed Forces transformation following NATO and the EU integration

Joining NATO and the EU were real historic moments for Romania and its armed forces. Being a member of such high-level international institutions influences the particular country's attitude and behaviour to increase self-confidence and trust in its partners, and to assume, voluntarily and consciously, important responsibilities regarding defence and security at national, regional and global level.

In fact, a member country of a powerful military-political alliance acts firmly to defend and promote national interests both domestically and externally, knowing that, if necessary, it is not alone but actually supported by its partners.

At the same time, national defence, for a member of a political-military alliance having the size of the North Atlantic Treaty Organisation, involves other dimensions and coordinates than for a country that does not have this particular quality.

The reform of the Romanian Armed Forces in the aftermath of NATO accession followed a path specific to the member states of a powerful political-military alliance that is internationally active. This can be seen analysing:

- *the structure and dimension of the large units and units in the armed forces services* – a new conception was implemented regarding the structure of military combat entities that met the requirements related to: flexibility, mobility and fire power, high capacity for self-sustainment and deployment in the theatre, reduced reaction time, capability to perform all the Alliance missions;

- *the size of the national armed forces* – a professional army was preferred, downsized, flexible and agile, to a mass, numerous one that is fixed in the field;
- *the location of large units and units on the national territory* – it was established following new criteria, proper to the armed forces of a political-military alliance member state;
- *the personnel education and training, and the armament and combat assets equipment* – are achieved according to the North Atlantic Alliance principles, norms and procedures;
- *the participation of some Romanian military structures in various missions outside the national borders* – the Romanian troops presence in international missions has been very important in the relations with NATO and the EU. Through their participation and, sometimes, their sacrifice, Romania has gained credibility, this way becoming an internationally recognised voice.

All these aspects prove that, at the level of the Romanian society and the one of the national armed forces respectively, it is conducted a continuous process meant to transform mindsets and habits towards mastering new patterns of behaviour derived from Romania's status of a full-fledged Alliance member state³.

For the Romanian Armed Forces, transformation is a process that allows for the strategic interests to be supported. The document that currently regulates this complex process at national level is the *Romanian Armed Forces Transformation Strategy*. It sets the goal of achieving a modern structure, fully professionalised, with a high degree of mobility, efficient, flexible, deployable, sustainable, able to act jointly and to be engaged in a broad spectrum of missions, both on the national territory and outside it⁴.

For this process development, *three phases* were established: *I. Completion of basic restructuring phase (2005-2007); II. Operational NATO and the EU integration (2008-2015) phase; III. Full NATO and the EU integration phase (2016-2025)*, which ensured/will ensure the achievement of transformation goals in the short, medium and long run.

The *second phase*, under development, has as main objectives: *to continue the readiness process for the forces earmarked for NATO and the EU; to complete the logistics system restructuring at strategic and operational level; to continue the procurement of new equipment as well as the major procurement programmes;*

³ Dr. Constantin Moștofleu, dr. Petre Dușu, *Apărarea colectivă și apărarea națională în contextul integrării României în NATO și al aderării la Uniunea Europeană*, Editura Universității Naționale de Apărare "Carol I", București, 2005, p. 31.

⁴ *Strategia de transformare a Armatei României*, București, 2007, pp. 15-16.

to reorganise military education; to systemically and structurally assess the main domains of the operational integration of the Armed Forces within NATO and the European Union and the substantiation of the decisions to correct and enhance policies, processes and ongoing programmes.

Main coordinates of the Romanian Armed Forces transformation in the medium and long term

The Romanian Armed Forces transformation is and will be conceived in the future in relation to the Alliance and the European Union transformation process.

Romania has clearly expressed its option regarding its membership in the Euro-Atlantic and European security structures. That is why the Romanian Armed Forces reform has to result in the establishment of a credible military structure, a modern, efficient, flexible, mobile one, able to act to accomplish the missions that are aimed at the defence of the country, the participation in collective defence and in multinational crisis management operations.

It is necessary, in this context, to highlight the most important premises that also determine the main coordinates of the Romanian Armed Forces transformation in the medium and long term.

The global, European and national security framework currently undergoes a profound process of structural changes and transformations that, through the scope and immediate and predictable effects, radically changes the political configuration of the continent, the nature of the relations between European states and in the geostrategic and geopolitical area Romania lies in.

The changes occurred in recent years in the international geopolitical context have highlighted a future scenario, characterised by more instability and conflicts, according to which a series of new threats, asymmetric ones, military and non-military, tend to increase as far as the degree of danger and the probability of occurrence are concerned.

The geostrategic area in the vicinity of Romania is very dynamic and fluid, the premises of potential conflicts coexisting here. In these circumstances, until a viable general European security system is established, Romania needs to ensure national defence, to safeguard the fundamental values and security interests, both through its own forces and means and through the ones proper to collective defence, concomitantly with meeting its obligations in the Euro-Atlantic area.

It is necessary to identify the similarities and differences between the general issue of NATO transformation and the transformation of the Romanian Armed Forces. In this context, the Romanian Armed Forces have coherently defined

a reform programme, more precisely a reconstruction one, on bases that are similar to those of NATO, having priorities related to available resources. This extensive process requires not only permanent information and responsiveness to the changes in the security environment, but also the ability to cast aside the obsolete concepts and conceptions, easily, without efforts and psychological imbalances, to courageously put the new ones in practice, with reasonable financial and logistic costs, and especially with efficiency⁵.

Collective defence and security, specific to NATO, and security based on cooperation and the use of non-military instruments, specific to the European Union, although they are fundamentally different instruments of international security policy, are, nevertheless, complementary to ensure stability and security in the European area.

The Union's ambition to become an "actor" in the global arena has direct implications on not only the member states security and defence policies but also on the transatlantic relations, between the EU, NATO and the USA.

During the past 15 years, NATO has transformed from a military alliance and a collective defence system oriented towards the Euro-Atlantic area into an organisation meant to maintain peace and international stability, to manage crisis, to prevent conflicts, to reconstruct and stabilise the areas affected by conflict, absorbing more of the objectives, responsibility and the logic of some bodies that had proved unable to yield order and security.

At the same time, NATO continues the restructuring process – its capabilities have to be transformed, and its forces must become lighter, easily deployable, agile and expeditionary, its institutional structure has to be changed and an entire portfolio of political dialogue with its neighbours has to be opened. Practically, during this whole process Romania has participated in as an associate, candidate, member and full-fledged member, NATO has become a different organisation.

Its evolution does not end here. The guidelines for the transformation of the Alliance and the Romanian Armed Forces are in the process of being issued after the *new strategic concept* is drafted. The deadline for the document completion was the NATO summit in Portugal, in November 2010.

NATO Deputy Secretary General mentioned five main themes to be approached in this context, as follows:

- *the relation between Article V operations (collective defence) and non-Article V operations;*

⁵ General dr. Mihail Popescu, *Planificarea – funcție determinantă în reducerea duratei ciclului conducerii acțiunilor militare întrunite*, Editura Militară, București, 2002, p. 8.

- *the significance of the solidarity principle in the context of new types of risks (cyber attacks, energy insecurity etc.);*
- *the future of NATO partnership relations, the relations with Russia included;*
- *aspects regarding communications;*
- *public diplomacy*⁶.

Prior to the Summit, Romania expressed its proposal that in the final form of the *new strategic concept* should be also found other important elements, such as strengthening NATO interest and developing cooperation with the partners in the immediate vicinity of the Alliance and of Romania, in Western Balkans and the Wider Black Sea Area, including the South Caucasus and Central Asia, and enhancing NATO's partnership network and maintaining the Alliance's enlargement policy ("*open door policy*"), which made a significant contribution to strengthening stability and security in Europe⁷.

The Romanian Armed Forces will continue, also in this context, the transformation process. In the medium and long term, the implementation of concepts, organisational structures and new equipment will take place following coordinates that are, in part, established, but the dose of unpredictability is inherent in a process conducted over a long time horizon.

We have primarily in mind to meet the objectives set by the *Transformation Strategy*. It is a defining process to modernise the armed forces, which has undoubtedly ensured a qualitative leap in the evolution towards a modern and efficient army.

Concurrently, we have to mention the evolutions that are difficult to predict, determined by the different economic and social development, the emergence of risks and threats that have new forms of manifestation or that are extremely violent, important technological "*leaps*" etc., which will lead, as far as the military body is concerned, to the adoption of solutions that cannot be taken into account at this moment.

The political and military factors with responsibilities in the field of defence planning have a key role in establishing the general issues of the armed forces transformation and the fundamental elements that lead to the development of medium- and long-term strategies.

The force sizing issue should not be based on purely theoretical, subjective or situational considerations. It has to be addressed and resolved taking into account the Romanian realities, national interest, the physiognomy of a possible military conflict and the necessary potential for a strong and credible response, as well as the dramatic evolution in waging war, proven by recent military events.

⁶ At <http://www.juridice.ro/87906/nou-concept-strategic-al-nato.html>

⁷ At <http://www.mae.ro/index.php?unde=doc&id=40765>

In the general transformation process, the conceptual aspect represents an objective necessity, a reaction to adapt to the structural changes that will occur in the Romanian Armed Forces and within the North Atlantic Alliance.

Military transformation represents a continuous process of development and integration of new concepts, strategies, doctrines and capabilities in order to improve efficiency and the degree of forces interoperability and of adapting to the new constantly changing security context, which highlights the need for reevaluating the military factor as the main source of credibility. This requires changes in doctrines, organisation and force structure, capabilities, intelligence activities, training, education and procurement, personnel management and phasing based on programmes, which become the main areas that must undergo transformation⁸. *The organisational evolution of the Romanian Armed Forces will have to be included in the directions of development defined at the European and Euro-Atlantic level.*

As far as *command structures* are concerned, mention should be made that, at the Alliance level, a series of analyses was initiated aimed at reconsidering their organisation with a view to optimising the act of command, shortening the reaction time and ensuring a better relationship between decision-makers and performers.

Some of the conclusions that are specific to joint commands should be mentioned here, as they represent reference points regarding the establishment of the future coordinates of the command structures at the level of our armed forces.

The proposed organisational structure has taken into account two elements: a main module, which comprises the majority of the personnel, and a deployable, more reduced, one. The main module consists of a command group (command and command team) and 3 components: operations, resources and training. The operations component may include a joint operations centre, joint plane microstructures, joint assessments, synchronisation and execution, effects management and intelligence. The resource component may have human resource, logistic, financial, medical, engineer, communications and information microstructures. Also, the training component may have training and lessons learned microstructures.

The deployable module does not have to be understood as a command one. It is because it is a part of the joint command and not an additional command level. A structural solution, more flexible and oriented towards the main domains that have to be managed, more adaptable rather than oriented towards the specific needs of a certain type of command is thus taken into account.

⁸ *Strategia de transformare a Armatei României, op. cit., p. 12.*

As for the *combat structures*, in order to establish the coordinates for the medium- and long-term evolution, both the current solutions, identified at the alliance or national level, and the development paths that emerge from the conducted analyses and studies or the lessons learned in the theatres of operations in the last years should be taken into account.

Not only at this moment but also in the future, at the EU level, the *battle group* is considered the basic structure that may be deployed and sustained in a theatre of operations. It consists of about 1 500 troops, it is held at a readiness of 5-10 days, and it should be self-sustainable for at least 30 days, extendable to 120 days if re-supplied appropriately.

The operational force of the Alliance is *NATO Response Force (NRF)*, which is a highly ready and technologically advanced force made up of land, air, naval and special forces components that can be rapidly deployed wherever needed. Its strength is up to 30 000 troops, it may be deployed within five days since notification and it is self-sustainable in operations for up to 30 days or even more if appropriately resupplied.

The USA implements the transition from an army based on division echelon structures, meant to fight in one or two major theatres of operations, to one based on brigade-level structures, standardised, self-sustainable, having a strength of 3-4 000 troops, more types of branches, expeditionary and deployable anywhere in the world.

Other countries in the world that have powerful armies approach the transformation of the military structures organisation in a similar manner.

The analysis of these options in the field of structure highlights their common element represented, in our opinion, by the need to organise structures as similar as possible to the way they conduct fight, downsized but having a high reaction capacity and firepower.

Consequently, we appreciate that, at the level of our armed forces, the organisational structure of the divisions and brigades in the land forces should be reconsidered so that they become groups of forces able to take action independently, for longer periods of time, by including in their composition all the forces that currently are, conceptually, earmarked as strengthening or support forces. Stronger brigade-level artillery, engineer, reconnaissance, logistic forces, as well as division-level intelligence, aviation/helicopter and logistic forces are considered.

The increase in the firepower is closely connected to the armed forces procurement and modernisation process. It is aimed at modernising the structure of the armed forces through personnel reduction and procurement of new and enhanced technology, compatible with NATO standards.

The importance of a rapid and effective reaction should be also reflected in the *types of structures* in the Romanian Armed Forces. The current way of constituting deployable, generation and regeneration forces⁹ is already the subject of the analysis of the experts that support another approach, too, as forces with a short, medium and long-term readiness.

Such an approach is compliant with the evolution trends at the European and Euro-Atlantic level. General Lance L. Smith, former Supreme Allied Commander for Transformation highlighted: *My top three priorities are deployability, interoperability and sustainment*¹⁰.

To meet them is the necessary condition for the future developments.

*

The Romanian Armed Forces transformation is a comprehensive, complex, multidimensional and continuous process that requires a profound conceptual reform, the command act optimisation, the structures reorganisation, their better coordination, and their functional integration in the security systems Romania is part of. Given the complexity of the phenomenon, it should be understood that a fundamental change can be achieved only in a longer period.

The military body reform should be continued not only because of the need for permanently accomplishing specific missions but also because of the existence of certain factors that determine this process, such as: Romania's participation in ensuring global and regional security, the access to technical, scientific and organisational novelties in all fields, the need to adapt to the evolution trends defined at the European and Euro-Atlantic level.

The Romanian military system transformation, in compliance with the democratic developments in our country and the challenges of contemporary security environment, requires the full engagement of all the intellectual, human, material and financial resources and it will allow to meet the set goal: to achieve modern, organised, properly trained and equipped armed forces, able to carry out, in the new security environment, the missions set by the Constitution.

English version by
 **Diana Cristiana LUPU**

⁹ Law no. 346 on 21 July 2006 regarding the Ministry of Defence organisation and functioning, art. 27 (1).

¹⁰ General Lance L. Smith, Supreme Allied Commander for Transformation, *NATO Continuous Transformation*, in *NATO Review*, summer, 2006, at <http://www.nato.int/docu/review/2006/an/interview.html>

THE JIHAD AND THE DYNAMICS OF GLOBAL SECURITY

Colonel (r.) Eugen LUNGU

The author begins through a short introduction regarding the new tendency for relating with the Islamic world, noting an element that has provided the new American Administration with increased credibility: the elimination of the syntagm “war against terrorism”.

Then, he makes an attempt to “decipher” the jihad – one of the most important concepts of the Islam. Moreover, he takes an approach to certain religious, ideological, military and political aspects regarding this concept.

In the end, he draws some conclusions from the perspective of the influence the “offensive jihad” has, as a means of violent action (the one promoted by the terrorist organisations that operate globally), on the global security environment.

Keywords: *jihad; Romanian National Defence Strategy; European Security Strategy; al-Qaeda; French White Paper on Defence and National Security; US National Security Strategy*

As far back as 1993, there was an idea in *International Herald Tribune* that the “Muslim fundamentalism is fast becoming the chief threat to global peace and security”¹. The spectacular changes initiated and promoted by the USA after 11 September 2001 in the field of global security through the operationalisation of the “war against terrorism” have reconfigured and influenced the security strategies for the United States of America, as a sole global superpower, as well as for the main regional actors, determined to reshape their strategies in this direction, the policies in the field of defence and the relations with some states of the Islamic world. In fact, it is well known that the “11 September attacks against the US have put the national security interests at the top of the American concerns (...). The terrorist threat has created not only the ground but also the opportunity for the Americans to confirm their willingness to use force against enemies”².

Colonel (r.) Eugen Lungu – *Lumina – Instituții de Învățământ* Foundation, București.

¹ The article is written by C. Hollingworth, in *International Herald Tribune*, 9 September 1993, republished in Sophie Bessis, *Occidentul și ceilalți*, Editura Runa, București, 2004, p. 251.

² Andrew Kohut, Bruce Stokes, *America împotriva lumii*, Editura Antet XX Press, Filipeștii de Târg, 2006, p. 213.

Thus, after these terrorist attacks, as well as in the period that followed, in the context of launching the military operations in Afghanistan and Iraq, prominent pundits in the field of global security reckoned that the USA has unilaterally enforced a new “*global policy*” regarding international security, seeking its own hegemonic interests, many times in disagreement with the vision of its Euro-Atlantic partners about managing global security.

Jihad and some Current Security Strategies

Identifying an enemy to hold the “*centre*” of the American security strategy, in the context of the return to a *real politik* established on relations of force between states, has been one of the notable elements of this approach of the USA: “*Redefining a global ideological enemy, in the continuation of the war against terrorism, and which is now Islamism, even Islam itself*”³. The day of 11 September 2001, beyond the tragedy it identifies with, is believed to have opened a new era in the field of global security, as the important security strategies drawn up after this day have listed Islamist-originated international terrorism as the most serious threat of the following years to global peace and stability. Although, after Barack Obama took office at the White House, one may talk of a visible change of attitude of the American Administration towards the Islamic world, security experts are further concerned with the response strategies of the Western world to the violent “*arsenal*” that Islamic fundamentalism, and especially terrorist movements, may display anywhere in the world. If, during the Bush Administration, launching the war against international terrorism, as well as against “*Islamofascism*” – as the Islamic threats was named in Washington – represented the main course of action in the USA to provide global peace and stability, the Obama Administration has promoted a different attitude since 2009, which consists in the improvement of the relations with the Muslim world. In this context, giving up the syntagm “*war against terrorism*”, considered by some authors as the expression of a real “*modern crusade*” against the Muslim world, has represented an element that provided the new American Administration with increased credibility. One can say that this attitude of the American Administration towards the Islamic communities, reflected in the official discourse and documents, shows that a new historical “*period*” has begun as far as the different way in which the perception, understanding and relation with the Islamic world is intended. One can even speak of imposing a “*different conduct*” in the official American *politically correct*-type discourse and documents, which avoid the use of certain expressions or words

³ Oliver Roy, *Semiluna și haosul*, Editura Nemira, București, 2010, p. 42.

that moderate Muslims consider to be insulting for the Islam. Recently, more precisely on 13 August 2010, American President Barack Obama expressed his agreement, in a speech at the White House, for the construction of a mosque and of an Islamic centre near Ground Zero – New York, on a private property in Manhattan, not far from the place of the two twin towers crushed down by Islamic terrorists on 11 September 2001. Obama stated that “*Muslims have the same right to practice their religion as everyone else in this country*”⁴. The President’s opinion, without a power of decision in this case, aroused many attitudes against it, especially on the part of the relatives of the almost 3 000 victims at the World Trade Center, yet, it is inscribed on different coordinated, namely to consider and treat differently the Muslim communities worldwide. However, it is worth mentioning that, even if syntagms such as “*Islamic terrorism*”⁵, “*Islamic fundamentalism*”, “*Jihadism*” etc. are no longer part of official White House documents, international terrorism with planetary implications is still perceived in Washington as a major threat to global security. The change in the attitude of Americans towards the Muslim world, regarding the desire to improve the relations with Islamic communities, does not however mean the manifestation of some “*weaknesses*” towards terrorist organisations, such as al-Qaeda, but quite the contrary. Both al-Qaeda – global terrorist organisation in support of violent Islamism – and other regional terrorist organisations that are doctrinally based on the interpretation of some Islamic concepts will definitely continue the “*Jihad against unbelievers*”, even if, in Washington, one can speak of a different American policy regarding the Islamic world. Therefore, even if a new way of understanding and approaching the Muslim world is anticipated in some states in the Euro-Atlantic community, one cannot let aside the fact that the fundamentalist movements and the Islamic terrorist organisation further represent a major factor that can cause insecurity at regional as well as global level. In this context, we believe it is elementary that people are aware of the fact that the correct understanding of the specifics of the Muslim world, of the concepts of Islam that are communicated in the rhetoric of Islamic fundamentalists and terrorists represents one of the most important elements that must be considered when drawing up the current and future security strategies.

After this short introduction regarding the new tendency for “*relating*” to the Islamic world, we intend to “*decipher*” Jihad – one of the important concepts of the Islam, to approach some religious, ideological and military, as well as political

⁴ At http://news.yahoo.com/s/ap/20100814/ap_on_go_pr_wh/us_ground_zero_mosque_obama

⁵ It can be noticed, from the content of the 2010 US National Security Strategy, that syntagms such as *Islamic terrorism*, *Islamic fundamentalism*, *Jihadism* etc. are no longer employed, in keeping with the new policy of the White House, attempting to normalise the relations with the Muslim world.

aspects regarding this concept and draw certain conclusions from the perspective of the influence exerted by “*offensive Jihad*”, as a means of violent action (the one promoted by terrorist organisations that carry out global actions), on the global security environment. We therefore intend to succinctly refer to certain aspects regarding “*defensive Jihad*”, “*claimed*” by Islamists who use war as an instrument for aggression, as well as by Islamist fundamentalists and Islamist terrorist organisations. Reading the *Qur’an*, one can notice that the Jihad is found in 35 verses, in which there are made general references to this concept, on the one hand, as a purely spiritual act of inwardness of a certain state and, on the other hand, as a “*conduct*” that is proper to Muslims in the armed confrontation. Moderate Muslims speak of the *Jihad* as a “*struggle with oneself*” to overcome all difficulties and temptations of daily life, as well as a defensive fighting “*means*” (*defensive Jihad*). Here are two reflections about “*defensive Jihad*”, considered a “*means*” to counter the enemies of Islam who resort to force: “*Jihad is an integral part of the concept of defending Islam. The primary meaning of the word Jihad is: to strive with all powers, to fight (...). According to the Sharia, namely the Islamic law, this word is used only to express the struggle waged for the name of Allah against the enemies of Islam who resort to force*”⁶; “*Jihad has been known as a source of conflict for 14 centuries, and Islamist apologists and members of academic communities claim that it allows only the defensive fight or even that it is nonviolent*”⁷; “*offensive Jihad*”, the second meaning given to the Islamic concept of Jihad, is based on an interpretation that Islamic fundamentalists, in particular, but also Islamist terrorist movements give to *Qur’an* verses on Jihad, in order to ensure connection and doctrinal consistency for these movements. Thus, some papers dealing with the concept of *offensive Jihad* start from the so-called “*verses of the sword*” (*Qur’an* verses that speak of Jihad as a means of armed fight) and aim at deciphering, interpreting and clarifying the Prophet’s reflections on the subject. Therefore, offensive Jihad has its origin in a different understanding and interpretation of the *Qur’an* on the phenomenon of war, compared with the so-called *defensive Jihad*, but this reflection is specific to a minority in the Muslim world – fundamentalist movements and Islamic terrorist organisations: “*For political reasons, to gain followers of the militant position, fundamentalists set out sacred obligations of the Qur’an and interpret abusively Qur’an texts to turn them into a battle flag*”⁸. For the individualisation of Islamist movements which promote offensive Jihad as a means of fight

⁶ Seyyid Ebul’A’ la el-Meududi, *Introducere în islam*, Editura SC Chrater SRL, București, 1991, p. 90.

⁷ Virginia Mircea, *Islamul și soarta lumii. Fundamentalismul islamic ca ideologie politică*, Editura Semne, București, 2009, p. 211.

⁸ *Ibid*, p. 209.

against non-Muslims, in a series of works outside the Islamic world there are used terms such as “*Jihadism*” and “*Jihadist movement*”, just to make a distinction between the Muslim minority supporter of “*aggressive Islamism*” (fundamentalist and Islamic terrorist movements) and the big mass of the Islamic world, supporter of defensive Jihad. In order to eliminate ambiguities, we mention that we will use in the continuation of our approach the terms “*Jihadism*” and “*Jihadist movement*” with the meanings mentioned above, precisely to ensure greater clarity, understanding and use of these concepts derived from Jihad.

We further intend to refer to certain security strategies drawn up in the latest years by the players that take action at global and regional level, as well as to the project of the *Romanian National Defence Strategy*, drawn up in June 2010, in order to observe the way in which terrorism as a global action is considered in these documents, the way in which this form of extreme violence, that claims its affiliation to Islam, manifests and what we believe it is required to be done from the viewpoint of global security in order to counter the actions developed by the terrorist movements that promote Islamic fundamentalism. The *European Security Strategy/2003* underlines the fact that the terrorist phenomenon, especially the “*al-Qaeda type*”-global terrorism, represents the first threat to member states: “*Europe is both a target and a base for such terrorism: European countries are targets and they have been attacked. Logistical bases for al-Qaeda cells have been uncovered in the UK, Italy, Germany, Spain and Belgium. Concerted European action is indispensable*”⁹. We can say now that the European Union’s security strategy, developed in 2003, and followed, unfortunately, by the terrorist activities in Madrid and London confirmed that defining terrorism as a first threat to community states was based on properly grounded analyses. Moreover, the Report on the implementation of the *European Security Strategy* on 11 December 2008, developed precisely to strengthen this strategy, addressing key global challenges and threats to security, has once again shown that terrorism is a major threat to Europe: “*Terrorism, within Europe and worldwide, remains a major threat to our livelihoods. Attacks have taken place in Madrid and London, while others have been foiled, and home-grown groups play an increasing role within our own continent*”¹⁰. Another reference document – the *French White Paper on Defence and National Security/2008* – finds global terrorism generated by radical Islamist movements as a major threat

⁹ *European Security Strategy*, Brussels, 12 December 2003, p. 3, at <http://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf>

¹⁰ The report on the implementation of the *European Security Strategy – Providing Security in a Changing World*, Brussels, 11 December 2008, p. 4, at http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/RO/reports/104652.pdf

to Europe. We note that this document is one of fundamental importance for the security of France, including benchmarks for the European security environment, direct references to the concept of Jihad, thus proposing a more careful analysis of the elements that define the “religious dimension” of global security. Starting from a wide range of possible risks and threats, the Paper contains references to “defensive Jihad”, a concept without aggression and specific to moderate Muslims, as well as considerations about “offensive Jihad”, characteristic of fundamentalists and Islamic terrorist movements: *“In Europe, Jihad is often translated as <holy war>. Etymologically, though, Jihad signifies <an effort towards a specific goal>, i.e., on the one hand, the effort to defend or spread Islam, and on the other, an effort on the part of the believer to conform to the rules of the Qur’an. This reference appears in various verses of the Qur’an in different forms: spreading Islam by persuasion, fighting to repulse an attack on Islam etc.”*¹¹. Moreover, the French document also refers to the concept of “Jihadism”, which has a negative significance in the Western world and, in general, in the non-Islamic world: *“Just as one distinguishes Islam from its political exploitation (“Islamism”), one needs to distinguish the religious notion of Jihad from “Jihadism”, which is a deformation of it through terrorist action”*¹². Unlike the French Paper, the *US National Security Strategy*, completed in May 2010, has a different approach from the viewpoint of defining the Islamist threat, namely in consensus with the principles the Americans currently promote in order to improve their relations with the Muslim states. The document is different, from this point of view, from the one drawn up by the previous Administration, clearly showing that the Christian world is not at war with the Islam and eliminating the syntagm of “Islamic terrorism”, often used before. The stated objective of President Barack Obama to improve the relations with the Islamic world, expressed ever since he took office, can also be found in the *National Security Strategy*: *“We are developing new partnerships in Muslim communities around the world on behalf of health, education, science, employment, and innovation. And through our broader emphasis on Muslim engagement, we will communicate our commitment to support the aspirations of all people for security and opportunity. Finally, we reject the notion that al-Qaeda represents any religious authority. They are not religious leaders, they are killers; and neither Islam nor any other religion condones the slaughter of innocents”*¹³. Moreover, the same document reminds us that the syntagm

¹¹ *Défense et Sécurité Nationale, Le livre blanc*, Paris, 2008, p. 28, at http://www.livreblancdefenseetsecurite.gouv.fr/IMG/pdf/livre_blanc_tome1_partie1.pdf

¹² *Ibid*, p. 27.

¹³ *US National Security Strategy*, May 2010, p. 22; at http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

“war against terrorism” was given up, an idea expressed by President Obama shortly after taking office: “We will always seek to delegitimize the use of terrorism and to isolate those who carry it out. Yet this is not a global war against a tactic – terrorism or a religion – Islam. We are at war with a specific network, al-Qaeda, and its terrorist affiliates who support efforts to attack the United States, our allies, and partners”¹⁴. Therefore, *US Security Strategy*, although it no longer contains phrases like “Islamic fundamentalism”, “Jihadism”, “Islamic terrorism” etc., for the reasons mentioned above, refers to the “al-Qaeda”-type global terrorism (the one that, as its leaders state, promotes the “*jihad against the unbelievers*”), which is considered as a serious threat to global security. Even if this important document for US security and global security does not contain phrases considered offensive to the Islamic world, we believe that combating the terrorist organisation al-Qaeda and other terrorist organisations which establish their actions, in terms of doctrine, on the interpretation of concepts of the Islamic religion, will also take into account the meaning of the concept of Jihad, as well as the power to psychologically influence the messages that contain this term. As regards NATO’s future approach to the international terrorist phenomenon, including the insecurity generated by the Jihadist movements that undermine the security interests of the Alliance, it is known that the group of 12 experts from various member states, led by former US Secretary of State Madeleine Albright, presented, in May 2010, in Brussels, recommendations regarding *NATO’s New Strategic Concept/2010*, a key document for the Alliance, which was adopted this autumn at the Lisbon summit. In the report, it is stressed the importance of Article 5 of the North Atlantic Treaty on the indivisibility of collective security, in which there are mentioned the “*non-conventional threats*” that are maintained for allies (terrorist attacks, weapons of mass destruction, cyber attacks etc.) and, from this perspective, it is suggested that, in the future, the Alliance will continue to take action outside the traditional area of responsibility. It thus follows that, alongside the other threats, international terrorism continues to be one of the important unsecuring elements that NATO will counter in the coming years, in keeping with the *new strategic concept* that will be operational in the final part of 2010. Certainly, starting from the requirements of the new strategic concept, the Alliance will continue its process of structural transformation and of provision of new weapon systems and military equipment in order to effectively meet the full range of threats, including the terrorist threat. The draft of the *Romanian National Defence Strategy*, discussed in the Country’s Supreme Defence Council on 22 June 2010 and submitted to the Parliament, also shows the phenomenon

¹⁴ *Ibid*, p. 20.

of international terrorism as the most important threat to Romania: *“The expansion of the ways of manifestation of terrorism at international level, through the diversification of the base of support and recruitment, as well as the emergence of new risks arising from religious radicalisation, cyber terrorism, or virtual propaganda”*¹⁵. It can be noticed from the content of the document that the draft of the *Romanian National Defence Strategy*, as well as the proposals for *NATO’s New Strategic Concept* do not contain explicit references to *“Islamic terrorism”*, *“Jihad”* or *“Islamic fundamentalism”*, but there are used other words, as *“religious radicalisation”* or *“international terrorism”*. In the same spirit, expressed by the adoption of a positive attitude towards Islam, resembling to the one of the Obama Administration, other countries in the Euro-Atlantic world will also try to adapt their documents and official discourse regarding the Islamic world. Thus, blaming all the Islam world will be avoided, as it unfortunately happened many times in the past years. The Euro-Atlantic community will have to remove the excesses of speech regarding Islam and to consider a very simple thing, that Islamic terrorism is caused by a minority of this world. This does not mean that some Islamic terrorist organisations will not be considered to be threats to global security, but, quite the contrary, they will be treated as such as long as the analyses of the risks and threats to global security will indicate so. Considering that we can much easily understand the religious issues that may lead to violence, in a context in which political, ideological, economic, military factors etc. play an important role, we will still use the concepts of *“Jihad”*, *“Jihadism”*, *“Islamic terrorism”* etc., taking into account the relation of these terms with the domain of global security. Thus, violent Islamism, which promotes offensive Jihad, specific to a small number of people, as shown in some of the documents summarised above, will definitely be considered in future years an asymmetric threat to democratic states. We believe that *“deciphering”* the phenomenon of the belligerence existing in the Islamic world, as well as the violence of the Islamic terrorism, will need to consider the way in which the religious, political, ideological elements are combined in the same radical Islamist movement, as well as the way in which violence occurs. Here is what journalist Sophie Bessis writes about the political and the violent *“sides”* of the Islamist movements: *“The question of the links between terrorist movements and the groups that have chosen a legal way to get to power is complex. It stirs spirits ever since the occurrence of the contemporary Muslim radicalism in the late seventies, and the Algerian drift from the nineties. Born from the same ideological matrix, fighting for the same conviction to establish*

¹⁵ *The National Defence Strategy – For a Romania that Guarantees the Security and Prosperity of Future Generations*, Bucharest, 2010, p. 13, at <http://roncea.ro/wp-content/uploads/2010/06/Strategia-Nationala-de-Securitate-a-Romaniei.pdf>

*the Islamic state, they have often been the two sides of the Islamist coin, the first being, more than once, the armed arm of the other*¹⁶. This existential complexity of terrorist movements, such as the al-Qaeda, in which the extremist political, religious, ideological and military ideals blend, makes the “*theme*” of countering these movements not simple at all within the framework of security strategies at regional and global level. We believe, from this point of view, that the development and implementation of viable strategies to counter and combat the phenomenon of international terrorism, which claims its Islamic origin, will have to consider a decisive and effective action, starting in several areas: political, diplomatic, military, economic, religious etc.

Jihad and the Dynamics of the Global Security Environment

Analysing the influences that Jihad may have on global security, to understand more thoroughly the mechanisms and reasons of Jihadist movements, we often come back to the Huntingtonian concept of “*clash of civilizations*”. In this regard, I would like to quote Mark Sedgwick, specialist in terrorism: “*The cultural conflict between the Muslim and the Western world exists but it alone cannot explain the clash of civilisations. One should pay attention to geography, history and politics in equal measure*”¹⁷. It is easy to say that Sedgwick is not right, but just as easy is it to say that what this author claims is a fact confirmed by the events currently underway in Afghanistan, Iraq, Lebanon etc. But we agree with many authors who say that Islam, same as Christianity and other religions, does not “*organically*” produce violence, as shown by the ancient history or the recent historical facts: “*Islam, the religion practised by Muslims (or Moslems) has been frequently stereotyped in European and North American political discourse, especially at times of conflict, such as the 1973 oil embargo, the 1979 Iranian revolution, the 1991 Gulf War, and the period since the 2001 terrorist attacks on the United States. Islam is no more conflict-prone than other religions, although Christian-Muslim conflicts are taking place in a dozen locations*”¹⁸. The Islamic terrorism, which is often referred to in the past years, according to experts in the field, has its beginning in the late '70s, with the US embassy hostage crisis in Iran.

Because radical Islamist movements began to carry out terrorist attacks especially in recent decades, it is clear that this type of extreme violence is caused by other extra-religious factors, among which the political, economic and military

¹⁶ Sophie Bessis, *op. cit.*, p. 249.

¹⁷ Mark Sedgwick, *Islamul și musulmanii*, Editura Niculescu, București, 2010, p. 286.

¹⁸ Joshua S. Goldstein, Jon C. Pevehouse, *Relații internaționale*, Editura Polirom, Iași, 2008, p. 263.

factors are definitely worth being taken into consideration. Therefore, although very different, the Christian religion and the Islamic one do not promote extreme violence when they become “neighbours” or are “associated” in that they would be in a certain “competition”. Violence is generated, we believe, not by the fact that the two religions would have a certain “origin” that makes them irreconcilable, but because there are many political and military problems of the Muslim world in whose “solution” there are involved, directly or indirectly, important western states belonging to the Christian cultural area. We believe that today there can be no conflict between civilisations in the Huntingtonian sense, although it is known very well that numerous Christian and Muslim “forces” do not spare themselves in the theatres of operations in Iraq and Afghanistan. However, starting from the reality of these military confrontations, from the large number of states engaged declaratorily, as well as from the informal participation of other countries (especially from the Muslim world), the advocates of the theory of the “clash of civilisations” have enough tangible arguments to speak of an “ongoing conflict” between the Christian and the Islamic world, pointing out, first, the religious aspects of the belligerence, and then the political ones. Against this background, the Islamic fundamentalist movements promote the Jihadist views as the only way to defeat the non-Islamic.

As I showed before, the concept of Jihad, in its offensive meaning, is connected to Islamic fundamentalist movements and Islamic terrorism. Nearly a decade after the tragic terrorist events of September 2001 in the USA, when global security studies unequivocally show that terrorism is a global threat to the security of states, the theme of Jihad attracts attention regularly. In this context, from time to time, al-Qaeda terrorist organisation, a “deterritorialised and global organisation”¹⁹, through its leaders, urges the populations belonging to this religion to the “holy war” against Westerners and all those who participate with troops in military operations in Iraq and Afghanistan, to try to influence the international public opinion regarding the capacity to act globally and to mobilise Muslims everywhere. Here are two fragments contained in the threatening messages sent by Osama Bin Laden in the name of Jihad against the West: “We do our duty of fighting for the sake of the religion of Allah. It is also our duty to send a call to all the people of the world to enjoy this great light and to embrace Islam and experience the happiness in Islam. Our primary mission is nothing but the furthering of this religion”²⁰;

¹⁹ Oliver Roy, *op. cit.*, p. 113.

²⁰ Michael A. Palmer, *Ultima cruciadă. Americanism versus islamism*, Editura Curtea Veche, București, 2010, p. 193.

“We believe that America is weaker than Russia and from what we have heard from our brothers who waged Jihad in Somalia, they found to their greatest surprise the weakness, frailness and cowardliness of the American soldier. When only eight of them were killed they packed up in the darkness of night and escaped without looking back. After this, a great stir has comprised the humanity regarding the new world order. People can, if they fear God – those who believe in His power, wage Jihad and who knows the current situation needs the right conditions. God knows everything”²¹. (Interview for the Al Jazeera TV station/1998 after the terrorist bombings in Kenya and Tanzania). In fact, looking at some of the texts sent by Islamist terrorist organisations, such as those of al-Qaeda, some authors who are familiar with the religious particularities of the Muslim world believe that many messages sent by these organisations differ a lot, willingly or not, from the Qur’anic meaning that moderate Muslims attribute to certain religious concepts. Thus, although this aspect is obvious in recent years for terrorist organisations included in the so-called “global terrorism”, we state that this phenomenon was also present in the past century: “In the last decades of the twentieth century, a kind of Islamic terrorism appeared, which is in direct contradiction with all the moral precepts drawn from the Qur’an”²². Although “the Jihads preferred by al-Qaeda troops were Afghanistan, Bosnia, Chechnya and Kashmir”²³, this terrorist organisation, through its leaders, keeps expressing its option for Jihad as a main “means” to defeat the western unbelievers. We believe that the fact that Samuel Huntington has a large number of supporters in the Western world, with the well-known concept of “clash of civilizations”, could be an advantage for al-Qaeda, which somehow embraces this thesis as true, thus obviously resulting the need for generalised Jihad to defend Islamic values. In this respect, this terrorist organisation does not intend to conquer or rule over a territory, but to produce, through its action, a “coup d’image” with global impact, to bring together the Muslim world against all those who are against Islamic values and disdain them. The existing conflicts (Iraq, Afghanistan etc.) are very important for al-Qaeda strategies, conflicts involving different Muslim populations who it would like to reorient, in the meaning of the “reconfiguration” of the phenomenon of belligerence (changing the composition of the camps in conflict, clarifying the religious belonging of fighters etc.), depending on the nature, particularities and interests of the Muslim world that al-Qaeda militants want to represent and to consider, despite its diversity and complexity, a world

²¹ *Ibid*, p. 191.

²² Irina Paladi, *Factorul islamic în relațiile internaționale*, article published in *Revista AXA*, 21 March 2010.

²³ Oliver Roy, *op. cit.*, p. 113.

with convergent objectives. Al-Qaeda “wants to parasitise the existing conflicts in order to give them a different meaning: the global Jihad against the West (...). Al-Qaeda needs those who demonise it, because, once again, perception leads to political action”²⁴.

*

Jihad, in its defensive meaning, is not a concept that should worry the world, in general and the Christian world, in particular. It cannot lead to global insecurity, because it refers, in religious terms, as it is perceived by most Muslims, to the defence of Islamic territories against those who want to conquer them. Moreover, the UN Charter recognises the right of states to self-defence, and the fact that a religion with more than one billion followers stipulates this right in the Qur’an, under the form of a religious precept – *defensive Jihad*, is not/it should not be a reason for concern for the non-Islamic world. Yet, when we talk of *offensive Jihad*, things are much different. This form of Jihad is promoted by the Islamic fundamentalist movements and the Islamic terrorist organisations (like al-Qaeda), which, as everybody knows, although represent a minority of the Islamic world, through the actions they carry out, regionally and globally, claim that they represent the “*point of view*” of the entire Muslim world. Thus, “*Islamic terror, which makes the headlines daily* – says Fareed Zakaria – *is a large and persistent problem but one involving a small number of fanatics. It feeds on the dysfunction of the Muslim world, the sense of real or imagined humiliation at the hands of the West and easy access to technologies of violence*”²⁵. These fundamentalist movements, sometimes difficult to separate from the terrorist ones, because of their strong anti-Western spirit, have interpreted and distorted the *Qur’an*, in keeping with their own planetary “*vision*” proposing Jihad as the only means through which Muslims can defeat the “*unbelievers*” and which may impose Islam on a global scale. For this type of Jihad, promoted by terrorist organisations with global action, such as al-Qaeda, the civilised world will have to find viable security strategies in order to avoid the repetition, in the future, of terrorist operations like those in New York, Washington, London, Madrid and Moscow. Moreover, there are several authors who express a certain pessimism about the ability of some states to respond effectively in the future to the threat of global terrorism. In this “*perimeter of approach*” can be found Alexandru Lăzescu, the current President-General Director of the public television, who said, after the terrorist attack in Madrid, that “*This raises serious doubts on the ability of Western states, mainly from Europe, to face the pressures exerted by the unprecedented attack of the Islamic fundamentalist terrorism*”²⁶. A first step in finding effective strategies


²⁴ *Ibid.*

²⁵ Fareed Zakaria, *Lumea postamericană*, Editura Polirom, Iași, 2009, p. 32.

²⁶ Alexandru Lăzescu, *Democrațiile occidentale între “putinocrație” și terorismul islamic*, in *Revista 22*, 5 April 2004, at <http://www.revista22.ro/democrațiile-occidentale-intre-putinocrație-si-terorismulislamic-838.html>

to fight “*al-Qaeda-type Jihadism*” is the abandonment of the phrase “*war against terrorism*” launched by the Bush Administration after 11 September 2001 and the approach to global terrorism as a phenomenon which surely cannot be produced by Islam as a major global religion. The Western world is now more and more aware that al-Qaeda is “*an accident*” of the Muslim world, a terrorist organisation born also with the complicity of the West and that the further approach to terrorism in the spirit of the year “*2001*” (“*Islamism equals fascism*”) would be a big mistake. We also believe that the Western world cannot eternally promote an ongoing war (as the “*war against terrorism*” was intended at the beginning) against fundamentalism and terrorist (Jihadi) movements. Admitting that, in a low proportion, fundamentalism is proper to all religions, that terrorism is also reflected in non-Islamic cultural areas (for example, in the Basque Country), that there clearly are extra-religious causes that can generate international terrorism (political, economic, social etc. causes), we think that it would be beneficial for global security if the issue of international terrorism could be addressed differently, as compared with previous eras. The historical events and evolutions have demonstrated that showing constant inflexibility of positions expressed regarding some movements considered terrorist, hanging on to certain ideological clichés, resorting immediately to “*hard*” solutions, evading any possibility of dialogue, under the rule of the well-known reason – “*do not negotiate with terrorists*” – are elements that should be part of the “*lessons learned*” in the past decades and facilitate optimal decision making in the field of global security. Who would have believed 20 years ago that the Palestinian Hamas, considered by the West as a terrorist organisation, would be a dialogue partner with Israel and the Western world? It is known that, as far as terrorism experts are concerned, the Hamas, as well as the terrorism in Northern Ireland, for instance, belong to a so-called “*national terrorism*”, different from global terrorism, which is spread worldwide. Taking the example of Hamas, we can ask ourselves what will the main actors of global security attitude be in the following decades, probably in a multipolar world, towards Jihadist movements? If terrorist operations similar to those of 11 September 2001 happen again and “*a different kind of war against terrorism*” continues, one that is aimed at Jihadi organisations, will the solution of the negotiations be excluded, as in the case of the Hamas a while ago? From the perspective of the respect for cultural and religious diversity, as one of the important principles of liberal democracy, we believe that the Western world and the security strategies that are generated inside this world must provide the political, diplomatic, economic, social etc. ways and mechanisms to reduce the danger posed by Jihadist movements for regional and global security. One of al-Qaeda’s “*claims*” refers to the unresolved problems

of the Middle East and we believe that solving the Palestinian issue, for example, often present in the rhetoric of some leaders of Jihadist movements, could be a “barometer” that would measure, more precisely than ever before, whether Islamic Jihadism would later fall into decline or quite the contrary. We believe that although the US has opened a new “era” in the relations with the Islamic world, in the sense of formally ending to blame the Islamic religion and Muslim communities, as it happened immediately after the September 2001 terrorist attacks, the global security strategies will take into account the danger posed by international terrorist networks with global action such as al-Qaeda, whose members are declared to belong to Islam. What Michael A. Palmer says cannot be circumvented by the experts in developing security strategies, in the circumstances in which the Euro-Atlantic world began to better understand that terrorism characterises only a minority of the Islamic world, the one that interprets Islam differently, compared to moderate Muslims: “bin Laden belongs to Islam. His actions are in accordance with the interpretation he gives to Islam, an interpretation which, although not universally accepted by Muslims, is still a viable one”²⁷. Therefore, we have here, clearly, the natural motivation to try to better understand both the concepts specific to moderate Islam and those “distorted concepts” promoted by Islamist terrorist organisations. In this way, we believe that the approach taken by security specialists to develop viable and effective strategies can be facilitated. For these reasons, we think that the understanding of Jihad both from the Qur’anic perspective and as a “weapon” of Islamist terrorist movements that act globally can only be an element of real professional support in dealing with the global and regional security domain in which international terrorism which claims its membership to the Islamic world further remains a major threat.

English version by
 **Iulia NĂSTASIE**

²⁷ Michael A. Palmer, *op. cit.*, p. 221.

THE MARITIME DIMENSION OF COMBATING PIRACY OFF SOMALI COAST

Lieutenant Commander Laurențiu MEȘTERCA

In this paper, the author addresses the subject of counter-piracy in which the international community has taken a significant interest, since the significant increase in piracy off the Horn of Africa in the latter half of 2008. This paper's focus is on the maritime community's response, leaving aside other solutions to the menace, namely the ground initiatives, and the regional approach. It explains the efforts undertaken, by both civilian and military organisations, and highlights anti-piracy measures taken by the merchant shipping community as the first line of defence. Against the legal backdrop ensured by UNCLOS, this paper describes the role of naval forces in tackling piracy, reflecting the controversy surrounding the practice of using warships in this mission. After presenting the actors involved, it then explains the evolution of the counter-piracy efforts, the tactics used by naval forces, as well as the challenges that lie ahead.

Keywords: *counter-piracy operations; anti-piracy; Somali piracy; dhows; UNCLOS*

Motto:

Pompei (to Marc Antony and Octavius Caesar):

"... and I must

*Rid the sea of pirates ..."*¹.

Shakespeare, *Antony and Cleopatra*,

Act II/scene 61

A product of the Somali pirates, modern piracy, manifest in the international waters off the Horn of Africa, has seen a steep rise since the autumn of 2008. The phenomenon stems from Puntland and Central-South Somalia², entities which are not able to deal with it, unlike Somaliland, which has had remarkable achievements in the fight against piracy, "*catching pirates when they are in the process of organising themselves*"³. These efforts were also noted in the Report of the UN Monitoring Group on Somalia, issued in March 2010⁴.

A worrying aspect is that the Somali pirate attacks are not limited to the Gulf of Aden and the Somali Basin. They have widened from the southern end of the Red Sea to "*as far south as Mozambique and off the coast of India ... So, the entire Indian Ocean is becoming*

Lieutenant Commander Laurențiu Meșterca – Targeting Cell Head, Allied Maritime Command Northwood, United Kingdom.

¹ Shakespeare, *Antony and Cleopatra*, http://www.shakespeare-literature.com/Antony_and_Cleopatra/11.html

a problem of piracy”⁶. The extension of the pirate operating range is a result of the intensive use of pirate mother ships⁷ which ensures the necessary logistics for performing this type of actions. Additionally, the level of aggression has increased, while the ransom saw an estimated rise from 40 million USD (in 2008)⁸ to 60 million USD (in 2009)⁹.



Figure 1: A Pirate Action Group⁵

The payment of ransom even though it is considered as an encouraging factor by pirates, constitutes the only way for the ship owners to release their crews. There are different stances with regard to this aspect. The US wants to add the names of two high profile alleged pirate leaders to a UN sanctions list, but the UK opposes this move. The reasons behind this is that paying of ransom is not a criminal offence in the UK and that Britain is under pressure from ship-owners and seafarers who prefer the present system, which makes it possible for ransom to be paid for dozens of ships and their crews,

² Somalia has a federal structure that consists of 3 entities: Somaliland in NW (favouring the independence), Puntland in NE (favouring autonomy) and Centre-South Somalia, which falls under the authority of the central authority, called Transitional Federal Government (TFG).

³ Stig Jarle Hansen, *Piracy in the Greater Gulf of Aden*, Norwegian Institute for Urban and Regional Research, 2009, p. 30.

⁴ *Report of the Monitoring Group on Somalia pursuant to Security Council Resolution 1853 (2008)*, 10 March 2010, <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N10/246/89/PDF/N1024689.pdf?OpenElement>

⁵ A classical Pirate Action Group (PAG) is made up of the mother ship (*whaler*) and several, mainly two attack boats (*skiffs*). The fuel drums, which confers a large autonomy for executing attacks at very long ranges, as well as the ladders and grappling hooks used to get aboard the merchant ships are clear indicators of the intent to hijack merchant vessels (picture on <http://www.eunavfor.eu/2010/04/eunavfor-frigate-victoria-destroys-pirate-vessels>).

⁶ Admiral Mark Fitzgerald, Commander of the US Naval Forces in Europe and Africa, *Somali Pirates Spreading their Net further in Indian Ocean*, 26.03.2010, Xinhua.

⁷ The mother ship can be either a whaler or a vessel acquired from various hijackings. The whaler (see *figure 1*) usually leaves the coast towing the attack skiffs and forms the so-called Pirate Action Group (see *note 5*) in order to capture merchant vessels and take the crews hostages with a view to getting ransom. In case that the capture of the merchant vessels fails, the pirates will focus on smaller vessels (usually trawlers or wooden fishing vessels, called dhows) with a low value on the market and not worth negotiating with the owners for ransom. These are used as mother ships, offering the pirates the upside of blending in the shipping traffic and of the surprise attack that may occur anywhere, depending on the quantity of fuel in the tank of the captured vessel. Another modus operandi is to use the already hijacked vessels that leave the anchorages to go further out into the Indian Ocean and take their skiffs with them.

⁸ Ken Menkhaus, *Somalia – What Went Wrong ?*, *RUSI Journal*, vol. 154, no. 4, August 2009, p. 9.

⁹ *Somali Pirates Attack Large Japanese Oil Tanker*, AFP, 27.04.2010.

and many of the negotiations go through London¹⁰. Consequently, the UK does not see such payments as being illegal under international law, but, in accordance with the EU common position, it would not participate in such transactions¹¹.

An International and Regional Response

Despite the fact that the maritime response is not the most efficient solution to combat piracy, it has been the quickest choice chosen by the international community for limiting the phenomenon. Although it is unanimously recognised that solving piracy off Somalia requires a comprehensive approach, this paper will focus only on the maritime dimension, leaving aside the land initiative and the regional dimension. The maritime dimension does not need to be exclusively seen in terms of military involvement, but also from a civilian perspective, namely the shipping industry.

Confronted with the large scale of the phenomenon, the majority of the state actors affected by piracy took a stance, both individually and collectively, as members of international organisations or ad-hoc coalitions (UN¹², EU, NATO, Coalition Maritime Force – CMF¹³, International Maritime Organisation – IMO, INTERPOL etc).

Although the Somali pirates have operated with a relatively low intensity since 1991, the year of Siad Barre's regime collapse, which coincided with the outset of the Somali crisis, the international community began reacting to the pirate actions in 2007, and especially in the second part of 2008. Thus, in 2007, the capture of a ship chartered by World Food Programme (WFP) to ferry humanitarian aid to the impoverished Somali population and an increase in the pirate attacks prompted IMO and the UN Security Council attention. The latter issued Resolution UNSCR 1772/2007, which was followed by UNSCR 1814/2008, which urged the states to continue protecting WFP vessels¹⁴, a mission that was started

¹⁰ Paul Reynolds, *UK Blocks Sanctions against Suspected Somali Pirates*, 9 August 2010, <http://www.bbc.co.uk/news/world-africa-10917961>

¹¹ The European Union Committee of the House of Lords, *Combating Somali Piracy: The EU's Naval Operation Atalanta, Report with Evidence*, 14.04.2010, <http://www.publications.parliament.uk/pa/ld200910/ldselect/ldcom/103/103.pdf>

¹² The UN, based on an US initiative, urged the nations and the international organisations to create a mechanism for international cooperation with a view to combating piracy off the Somali coast. Hence, on 14 January 2009, the Contact Group on Piracy off the Coast of Somalia (CGPCS) was set up, being a forum that brings together all the stakeholders in order to facilitate and coordinate the counter-piracy effort. This group convenes triennially, taking note of the outcomes of the four subordinated working groups focused on: coordinating the maritime military operations, juridical issue, informing the shipping industry (Best Management Practices) as well as the public opinion.

¹³ Coalition Maritime Force (CMF) is a maritime force built around the USA, headquartered in Bahrain.

¹⁴ UN Security Council Resolution (UNSCR) 1814 (2008).

by France in November 2007. Consequently, Denmark and subsequently Canada, the Netherlands, NATO, and the EU offered to carry on this effort.

In the context of an amplifying phenomenon, in the second part of 2008, the UNSC issued a series of resolutions initially requesting the member states to help combat piracy and armed robbery off the Somali coast (UNSCR 1816), then to deploy warships in the area (UNSCR 1839). The first response came from CMF, followed by NATO and the EU. In August 2008, CMF directed some of the ships belonging to Task Force 150 (TF 150) to patrol in the Gulf of Aden in order to protect merchant shipping. In order to render the patrol more efficiently with a limited number of warships, the CMF commander set up the Maritime Security Patrol Zone¹⁵. All the civilian vessels transiting the Gulf of Aden were advised to sail through the zone for their own safety. At the moment of getting involved in counter-piracy, CMF took advantage of the wide mission spectrum and the vast area of responsibility (Gulf of Aden, Gulf of Oman, the Arabian Sea, the Red Sea, and the Indian Ocean). However, the involvement in combating piracy was not favoured by all the nations contributing warships to TF 150, since this mission was not specifically listed in the mandate of the operation which chiefly has a seaborne counter-terrorism profile. This restriction was more or less of a political nature, depending on each nation's flexibility to respond to the new challenge in the Horn of Africa. In order to overcome this challenge, the states which were prone to combat piracy and did not wish to place their units under NATO or EU command, came up with a proposal to establish a new Task Force, named TF 151, dedicated to counter-piracy operations, under the aegis of the CMF, at the beginning of 2009.

Similarly, toward the end of 2008, NATO and the EU sent their own TFs in the Gulf of Aden. From 24 October to 12 December 2008, the Alliance temporarily deployed Standing NATO Maritime Group 2 (SNMG 2) to ensure the protection of WFP ships and merchant vessels that were transiting the area. The operation was dubbed "*ALLIED PROVIDER*" and was run by the Maritime Component Command (MCC) Naples. The protection mission of the WFP ships was handed over, in December 2008, to *ATALANTA*, the first EU naval mission conducted under the aegis of the European Security and Defence Policy (ESDP). Currently, this constitutes the main task of the EUNAVFOR, besides the protection of the vessels ferrying cargo for the African Union Mission in Somalia (AMISOM), and the deterrence, prevention and disruption of piracy. In the second part of 2008,

¹⁵ This zone was later replaced by the International Recommended Transit Corridor starting with February 2009, in Massimo Annati, *Non-Lethal Systems for Self-Defence of Merchant Ships*, Naval Forces, no. VI/2009, vol. XXX, p. 44.

all the BRIC¹⁶ states, except for Brazil, interested in the safety of their own merchant vessels and cargo in transit of the Gulf of Aden, sent their own warships to defend their economic interests. In this paper, from now on, the term *individual actors* will be used to name the participating states in the counter-piracy effort that do not contribute to the Task Forces belonging to the three main entities: NATO, the EU or CMF.

In January 2009, in the political context described above, CMF declared TF 151 operational, having as missions: deterrence, prevention and disruption of piracy. In March 2009, NATO resumed the missions off the Horn of Africa by deploying SNMG1, this time, the operation, code-named *ALLIED PROTECTOR*, being focused on the protection of the ships transiting the Gulf of Aden, deterrence, and disruption of piracy. The operation was run at the tactical level by the MCC Northwood, recently renamed Allied Maritime Command (MC) Northwood, while at the operational level it was run by Joint Force Command Brunssum. On 17 August 2009, the Alliance started a new operation – *OCEAN SHIELD*, simultaneously with the end of the *ALLIED PROTECTOR*.

OCEAN SHIELD is basically a continuation of the former operation, both in time and space, with the same actors but with two new elements. The first one is the comprehensive approach, which brings into play the institutional reconstruction at regional level in order to combat piracy, while the second element is the assumption of operational command by NATO's Joint Force Command Lisbon. The operation is in full swing, having, on a rotational basis, both SNMGs as the backbone of the Task Force 508 force structure, with the same command and control.

During 2009, many other warships were deployed by other individual actors from the Asia-Pacific area (Japan, South Korea, Malaysia, Australia and New Zealand). Among the regional states that are active in terms of presence can be cited Iran, Yemen, and Saudi Arabia. The number of warships involved in counter piracy is estimated to be “*on any given day ... some 30 to 40 warships ... from EU, NATO and the US as well as emerging Indian Ocean players China, Russia, India, Malaysia, South Korea and Japan*”¹⁷.

It is also worth mentioning that piracy is on the regional states agenda. Thus, in May 2010, at Abu Dhabi, during the “*Indian Ocean Naval Symposium*” (Indian initiative), 37 Indian Ocean coastal countries discussed the possibility

¹⁶ BRIC countries (Brazil, Russia, India and China) are deemed to all be at a similar stage of newly advanced economic development.

¹⁷ *Hi-tech Navies Take on Somalia's Pirates*, in *The Economic Times*, 16 June 2010, <http://economictimes.indiatimes.com/articleshow/6054828.cms?prtpage=1>

of conducting common counter-piracy operations. Separately, an Arab regional initiative [the United Arab Emirates (UAE), Egypt, Jordan, Kuwait etc.] under UAE direction¹⁸ started to take shape. Contributions to this initiative might consist of “*warships (the so-called Pan Arab Task Force), protection detachments, support, and suspected pirates prosecution*”¹⁹. The NATO Secretary General, Fogh Rasmussen, remarked that there is potential for extending cooperation in the fight against piracy with certain states within the Gulf Cooperation Council and with the partners in the Istanbul Cooperation Initiative (ICI). The NATO official launched the invitation to the ICI partners to participate in the NATO maritime operations, not necessarily with warships, but with support in the field of information, logistics, and exercises²⁰.

A Maritime Approach to Piracy

The maritime response against piracy can be seen as an interaction between civilian and military components.

The civilian component comprises the defensive measures, also called the *anti-piracy measures*, taken by the commercial fleets with a view to preventing the hijacking of vessels, deterring, and potentially disrupting piracy acts preventing pirates from gaining control of a merchant ship and hence buying time to enable military intervention if appropriate.

The military component comprises the naval forces engaged in counter-piracy operations in order to protect the merchant vessels, prevent, deter, and disrupt piracy acts.

It can be easily noticed that piracy prevention and deterrence are common to both components, but achieved differently. Thus, prevention can be achieved by merchant vessels by applying defensive measures, but also by the warships reacting to the SOS signals launched by pirate-threatened merchants. Similarly, deterrence can be achieved as a result of the presence of a security team onboard the merchant vessel or the presence of a warship. However, the prevention and deterrence, either conducted by military or civilian, cannot ensure a high probability of success against piracy.

The interface between the merchants and the warships is ensured by UKMTO (UK Maritime Trade Organisation Dubai) and MSCHOA (Maritime Security Centre – Horn of Africa), and not least the NATO Shipping Centre in Northwood. These are the points of contact for the merchants transiting the region that pass on the data

¹⁸ *Indian Ocean Navies to Seek Joint Anti-piracy Operations*, 06.05.2010, http://www.thaindian.com/newsportal/uncategorized/indian-ocean-navies-to-seek-joint-anti-piracy-operations_100359568.html

¹⁹ James Reinl, *UAE to Assess Role in Anti-piracy Task Force*, 15.05.2010, www.thenational.ae

²⁰ *Speech by NATO Secretary General A. F. Rasmussen on the Occasion of his Visit to the Kingdom of Bahrain, Manama*, 07.03.2010, http://www.nato.int/cps/en/natolive/opinions_62052.htm

(position and the ships vulnerability) about transiting vessels to the warships. In this way, the military component has a clear picture of the shipping traffic so that it can intervene in due time in case of pirate attack. Also, the warships can quickly warn the merchants when they detect the pirate presence. This exchange of information, absolutely necessary for achieving the *situational awareness* (SA), is done through a secured site owned by MSCHOA called *Mercury*.

❖ The Civilian Component

The working group 3, subordinated to the Contact Group on Piracy off the Coast of Somalia (CGPCS), destined to inform the shipping industry, has had an important role in pushing governments and the shipping industry to become aware of the piracy threat and to apply the necessary measures to prevent and deter pirate attacks. These are listed in the document (*Best Management Practice – BMP*) to prevent the piracy in the Gulf of Aden and the Somali Basin which reached the third version this autumn. It recommends registering ships with the UKMTO and MSCHOA, increasing the vigilance, executing manoeuvres, combined with an increase in speed in case of attack. Also, a series of passive protection measures (razor wire, electric fence etc.) and active measures (use of water hoses, non-lethal weapons and LRAD – Long Range Audio Device; Pain Ray) are recommended. It can be inferred that the use of specialised equipment has led to the development of a new market for manufacturers.

It has been noted that the majority of the captured ships ignored the BMPs, while their implementation paid off. In order to have more and more merchants putting these recommendations into practice it was signed “*The New York Declaration*”, in September 2009. Its signatories (the nations) committed themselves to enforcing the BMPs by the vessels flying their colours. To this end, the European Commission recommended the EU members to implement the BMPs in March 2010.

The anti-piracy measures quintessence was well captured by the former Danish commander of TF 150: “*The captain of the merchant vessel and her crew are the first line of defence for their own ship*”²¹.

In order to deter the pirate attacks, some ships have embarked armed personnel onboard, which can be private security teams (onboard the Spanish tuna fishing vessels) or military personnel (onboard the French tuna fishing vessels, vessels shipping weapons and ammunition etc). The presence of the private security teams, seen as a solution for the future²², needs to be authorised by the flag state,

²¹ Nathan Schaeffer, *Deterring Piracy at Sea*, All Hands, February 2009, p. 23.

²² Patrick Forestier, *Piraterie Maritime, Marine, Revue d'Information Maritime et de Défense*, no. 226, Premier Trimester 2010, p. 56.

in agreement with the ship owner and the operator. There are states that do not agree with this option (e.g. United Kingdom). These private teams are provided by specialised companies such as *Drum Resources Limited* – UK, *Secopex* – France, which earn substantial amounts of money (8 000 – 30 000 USD/day). However, these companies are perceived by some analysts as being “*lawless and seeking profits from fighting piracy... and it is another instance of private enterprise increasingly filling the voids of traditional state functions*”²³. The downside of having a security team on board is the possibility of escalating the violence during the pirate attack. A result of this was the killing, for the first time, of a pirate by a member of a security team²⁴. The incident took place on 23 March 2010 during which the guards onboard the Panama-flagged motor vessel *Almezaan* killed a pirate in a shoot-out between the guards and the pirates. The first question that comes out of this is: who is responsible for this? “*The state who hired the firm? The private shipping company that placed the guards on their boats? The private military firm employing the trigger-happy guards?*”²⁵. There is no clear answer since there is a judicial vacuum within the International Law.

There is another development that is taking shape – the private navies which might be seen operating by 2011 or earlier. These private maritime security companies (e.g. *Marque Star*) possess ships armed with deck mounted machine guns offering close protection for money for ships passing through the danger area²⁶.

❖ The Military Component

• The Role of the Naval Forces in Combating Piracy. The Legal Framework

Having in mind the environment where piracy gets manifest, warships have always constituted a handy tool for governments to suppress this menace. One of the historical milestones is Pompey’s suppression of the pirates’ fleet that threatened the Roman grain imports, following a naval campaign that lasted for 6 months. Similar examples continued over the centuries. As such, the Royal Navy was established to protect the British trading interests. Similarly, it is worth recalling that the establishment of the US warship fleet was more or less a consequence of having some of the US merchant ships captured by the Barbary pirates in 1785. Upon the building up of the US fleet, two naval operations were conducted in 1804 and 1815. The first one, known as the first war of America against terror²⁷, was concluded

²³ Shaun Randol, *The Lawless Fighting the Lawless*, 02.01.2009, <http://www.dmzhawaii.org/?p=1019>

²⁴ Katharine Houreld, *Private Guards Kill Somali Pirate for First Time*, 24.03.2010, AP, http://www.boston.com/news/world/africa/articles/2010/03/24/private_guards_kill_somali_pirate_for_first_time/

²⁵ Shaun Randol, *op. cit.*

²⁶ Peter Apps, *Are Panic Rooms and Private Navies Answer to Piracy?*, 4 October 2010, http://www.postchronicle.com/news/breakingnews/article_212325648.shtml?ref=rss

²⁷ Joseph Wheelan, *Jefferson’s War – America’s First War on Terror 1801-1805*, Carroll & Graf Publishers, New York, 2003.

with pounding the town of Tripoli and the release of the American hostages, while the second operation ended with the defeat of the pirates, which meant that the Barbary States (Alger, Tunis and Tripoli) had to pay compensation²⁸. Nowadays, the US takes into account the same risk, counter-piracy being considered a distinct mission to protect the US economic interests among the Navy peace missions²⁹. In spite of this approach, at the outset of Somali piracy, the majority of the nations did not have this type of mission for their navies. Consequently, some states, especially those that had their economic interests affected, adapted to the new risk, formulating counter-piracy as a new mission to be taken up by their navies.

The necessary legality of the warships to seize any ship captured by pirates and to arrest the latter is stipulated by the *UN Convention on Law of the Sea (UNCLOS)* adopted in 1982, at Montego Bay (Jamaica)³⁰. Also, the non-signatory nations of the UNCLOS are signatories of the precedent document – *Convention on the High Seas*, which has the same provisions regarding the interdiction of piracy, entitling any warship belonging to any country to combat the phenomenon³¹.

Although warships are authorised to retain pirates, in reality “most nations have junked archaic piracy laws and enacted no new ones”³². The legislation of some nations (e.g. Portugal) does not allow the prosecution of the pirates arrested in international waters³³. Other difficulties stem from the limited mandate of the international task forces, rules of engagement, transfer of pirates etc. In order to rectify these problems, in April 2010, the UN Security Council, in UNSCR 1928, urged all the states to view piracy as a crime in their internal legislation and to consider the prosecution of the suspected pirates and their imprisonment if found guilty.

• **Pros and Cons of Employing the Navies against Piracy**

There are controversies that surround the use of warships in the fight against pirates. On the one hand, there is a thesis that states warships should be used strictly for war tasks. A staunch supporter is Robert D. Kaplan, who sees the employment

²⁸ Melvin E. Lee, *The Fallacy of Grievance-based Terrorism*, Middle East Quarterly, Winter 2008, pp. 71-72, <http://www.meforum.org/1830/the-fallacy-of-grievance-based-terrorism>

²⁹ Milan N. Vego, *On Naval Power*, p. 8, in *Joint Force Quarterly (JFQ)*, issue 50, 3rd Quarter 2008.

³⁰ Art. 105, *UN Convention on Law of the Sea*, http://www.un.org/Depts/los/convention_agreements/texts/unclos/unclos_e.pdf

³¹ Roger Middleton, *Pirates and How to Deal with Them*, Briefing paper, Chatham House, 22 April 2009, p. 6.

³² Peter Chalk, *An Old Scourge Needs a Modern Solution*, in *The New York Times*, 3 September 2010, <http://www.nytimes.com/2010/09/04/opinion/04iht-edchalk.html>

³³ Joao Rebelo (Portuguese delegation), *Piracy on the Rise off Somalia*, 17.11.2009, NATO Parliamentary Assembly, <http://www.nato-pa.int/default.asp?SHORTCUT=1986>

of warships against the pirate skiffs as being an “*inefficient use of resources*”³⁴. Similarly, the American Admiral Mark Fitzgerald stated that the counter-piracy operations “*were limiting the number of US Navy ships available for other priorities ... in other areas ... It costs a lot of money to keep ships down there. It’s a lot of wear-and-tear on the ships themselves*”³⁵. Others deem that the naval response is nothing else than “*a pretext for training, an opportunity to improve the coordination with other maritime forces and a justification for their own budgets in a period when naval operations had a secondary place in the fight against terrorism*”³⁶. On the other hand, these theories are opposed with arguments of a political nature, the military presence off the Horn of Africa representing “*a political necessity ..., the public demands that the US and UK be perceived to be doing something to protect our economy*”³⁷.

I assess that doing nothing militarily to combat piracy at sea would obviously lead to the escalation of the pirate actions, which would be impeded only by the two monsoon seasons (during the winter and the summer) that make the sea too rough (impassable) for operating the pirate skiffs. In a more general note, the piracy issue is a good example for the relevance of the naval forces in the current setting of asymmetric risks to security, which dictates adaptation of today’s navies to the new reality.

- **Counter Piracy. Atypical Mission for the Navies**

It can be easily noticed the disproportionateness between the pirate and navy capabilities, an image reflecting the confrontation between David and Goliath (*figure 2*). On the one hand, there are the pirates on rudimentary boats (skiffs), armed with Kalashnikovs, ladders, and grappling hooks, while, on the other hand, there are well-prepared crews aboard state-of-the-art warships. If, on some occasions, pirates mistaken warships³⁸ for merchant vessels, once they deliberately attacked the USS *Nicholas* destroyer during the day (1 April 2010), an act that can hardly be explained. However, an explanation could be that the pirates are perceived as irrational actors due to the fact that they take khat, “*a drug which affects their state of mind*”³⁹.

Given that piracy is a crime, we are witnessing a policing mission, not a classic war operation, taken up by naval forces. Thus, the navies off Somalia “*are developing*

³⁴ Robert D. Kaplan, *Anarchy on Land Means Piracy at Sea*, New York Times, 12 April 2009.

³⁵ *Military Ships Can’t Stop Piracy*, Reuters, 16.04.2010.

³⁶ Ken Menkhaus, *Somalia – What Went Wrong ?*, loc. cit., p. 8.

³⁷ *Piracy Role Debated*, 14.01.2010, on www.sea-sentinel.com

³⁸ In the same situation were the military auxiliary vessels (DEU oil tanker *Spessart*, and the French command ship *Somme* – twice), and also the warships FRA frigate *Nivose* (France) and the HNLMS *Trump* (the Netherlands).

³⁹ Frank Gardner, “*Growing Risk of Deaths at the Hands of Somali Pirates*”, 4 October 2010, <http://www.bbc.co.uk/news/world-africa-11470238>

large human intelligence database from all the pirate suspects who have been captured, interrogated and released or charged ... backtrack [pirate GPS systems] logs to show the pirates origins⁴¹. In order to achieve this special tools are required such as "biometric tools to be able to keep records of the pirates"⁴². Consequently, the objective is not to kill pirates but to disrupt their actions and, when mandate allows, detain them in order to be transferred to right authorities



Figure 2: A Pirate Action Group intercepted by the boarding team. In the background the Greek ship *Limnos*, under NATO command⁴⁰

for prosecution. This effort requires catching the pirates red-handed, in parallel with evidence gathering for their incrimination. As a result, in this type of mission the weapons aboard the warships are used only in special situations: for warning or, in certain circumstances, for destroying the pirate paraphernalia.

• The Evolution of the Fight against the Pirates off the Somali Coast

In 2008 and the beginning of 2009, the naval effort was focused on the Gulf of Aden due to the higher density of traffic compared to the Somali Basin (approximately 560 vessels as opposed to 70 vessels per day) and the higher pirate propensity for this area. In order to enhance the security in the Gulf of Aden, an Internationally Recommended Transit Corridor (IRTC) was established⁴³. All the merchant vessels conducting passage in the GoA were directed to sail through the IRTC and were advised to use the group transit⁴⁴ so that they could enable the international task forces to conduct an efficient surveillance of the traffic by continuous patrolling of the IRTC by the warships. In order to efficiently cover the IRTC, given the limited maritime capabilities, the main three big actors (EU, NATO and CMF) resorted to the coordination of their efforts. This coordination is accomplished through monthly SHADE (*Shared Awareness and Deconfliction*)

⁴⁰ At <http://forum.keypublishing.com/showthread.php?p=1638392>

⁴¹ Chief of Staff to MC Northwood, Vice-Admiral Ort, quoted by Nick Brown, *Fighting the Hydra: Multinational Piracy Operations Move Inshore*, in *Jane's International Defence Review*, September 2010, p. 46.

⁴² <http://www.intelligenceonline.com/corporate-intelligence/2010/04/22/biometrics-for-pirates,83363193-ART-SEN>

⁴³ Internationally Recognised Transit Corridor consists of two corridors destined for transiting to west, respectively to east, each having the width of 5 nautical miles, separated by a buffer zone of 2 nm, having the length of 490 nm, and can be covered in two days at a speed of 10 knots.

⁴⁴ The group transit through the IRTC is based on passage speed. MSC HOA promulgates via their website, position, time, and speed for vessels to pass through a waypoint at the eastern and western limits of the IRTC. During the transit, the merchants should not expect to be permanently in company with a warship. However, all warships in the GOA will be aware of the Group Transit and will have the full details of vulnerable shipping. See www.shipping.nato.int and www.mschoa.eu.

meetings, the three organisations taking up the coordinator role of the IRTC, on a rotational basis. An important development is China's statement to cooperate with the three big actors⁴⁵. This move, besides providing more efficient patrolling, shows China's resolve to assume new responsibilities (aside from conducting escort duties) and signal that it is part of the club of the big naval powers.

Another form of protection of the merchant vessels, organised in convoys, is the escort. This is the characteristic mission of some of the individual actors (China, Russia, Japan, India) that accept in their convoys not only their own vessels but all transiting ships, regardless of the flag state. Even though the individual actors have been involved in their own escort missions, they have intervened to repel the pirate attacks when they have been in the vicinity of the ships that signalled a pirate incident.

The outcome of these efforts was reflected in a reduced number of the captured vessels in the Gulf of Aden in the second part of 2009 (only one ship captured in the last 6 months of the year). The key to success lay not only in an unprecedented coordination and cooperation of the main three actors (NATO, EU, and CMF), and the presence of the individual actors, but also in the application of the anti-piracy measures by the merchant vessels and a recent increased active involvement of the Puntland authorities in combating piracy on land.

Nevertheless, given the pressure exerted by the warships in the Gulf of Aden, pirates started conducting attacks at very long ranges from shore in the Indian Ocean, which equates to a massive area to be covered by warships⁴⁶. If the warships successfully covered the Gulf of Aden by patrolling the IRTC, covering the western part of the Indian Ocean with maritime capabilities to respond efficiently to any attack is a real challenge, given the limited resources⁴⁷. It must be highlighted that the IRTC remains the first priority, so that only the warships left available after IRTC coverage will be directed to the Somali basin. In order to paint a better picture of the challenge, Vice-Admiral Witthauer compared the area that needs to be covered by the TFs warships to the patrolling of France by 5 police cars⁴⁸. As for the long operating distance of the pirates using the mother ships, I assess that this is a direct consequence of the pirates speculating that the International Maritime Bureau recommended publicly that the merchant

⁴⁵ *China to Aid Somalia Anti-piracy Force: Diplomat*, AFP, 29.01.2010, <http://www.france24.com/en/20100128-china-aid-somalia-anti-piracy-force-diplomat>

⁴⁶ The area is approx. 2 000 000 sq. km., being 9 times larger than the Romanian territory.

⁴⁷ *Piracy on the Rise off Somalia*, 17.11.2009, NATO Parliamentary Assembly, <http://www.nato-pa.int/default.asp?SHORTCUT=1986>

⁴⁸ Vice Admiral Witthauer, Deputy Commander MCC Northwood, *Piracy on the Rise off Somalia*, 17.11.2009, NATO Parliamentary Assembly.

vessels sailed initially 200 nm, then 600 nm off the Somali Coast. Consequently, pirates increased their operating range to plunder right the IMB recommended area, currently reaching 1 200 nm. The very fact that these recommendations are posted on the Internet and they can be accessed by anyone proves the importance of the OPSEC (*operation security*) in the merchant shipping realm. Against this background, it is important for maritime recommendations for the merchants to be made in a secure way (logging on the sites dependant on password). The statement made by the EUNAVFOR spokesperson: “*The hijacking of the three Thai vessels (more than 1 200 miles off the Somali coast) was almost 600 miles outside the normal operation area for the EU Naval Force*”⁴⁹ basically constitutes an invitation for future similar actions. In order to strengthen this argument, the former EUNAVFOR commander, Rear Admiral Peter Hudson, stated that “*Pirates are adaptive ... and know that the distance will be a limit (for the naval forces)*”⁵⁰.

• **Modus Operandi of the Navies – Challenges**

In the fight against piracy, the success hinges on two essential factors: *Situational Awareness (SA)* and a high mobility. In order to get sufficient SA there is a need to locate and monitor pirate moves both on land and at sea. To this end, it is important to hold intelligence captured by *ISR (Intelligence Surveillance Reconnaissance)* assets, mainly airborne (Maritime Patrol Aircraft, UAV, helicopters), space sensors and submarines. In the future, there is the possibility that NATO will strengthen its intelligence gathering capabilities with AWACS⁵¹. Also, the Electronic Support Measures have an important role to play especially in terms of “*intercepting transmissions from mobile telephones and whatever radios and radars the pirates have*”⁵². Operation Ocean Shield was boosted (September-November 2010) by a Dutch submarine that was used in a “*covert inshore role*”⁵³, monitoring the pirate camps passing information to the maritime forces operating out at sea⁵⁴.

As for mobility, this feature is given mainly by seaborne helicopters that are able to react swiftly to the ISR feed or pirate attack.

⁴⁹ *Somali Pirates Seize 3 Thai Ships with 77 Crew*, AP, 21.04.2010, <http://www.reuters.com/article/idUSTRE63J30R20100420>

⁵⁰ *EU NAVFOR Defended in UK*, 14.01.2010, on <http://www.mschoa.eu/FairplayStoryDisplay.aspx?articlename=dn0020100114000007>

⁵¹ AWACS (Advanced Warning and Control Systems), *Piracy on the Rise off Somalia*, 17.11.2009, NATO Parliamentary Assembly, <http://www.nato-pa.int/default.asp?SHORTCUT=1986>

⁵² Chief of Staff to MC Northwood, Vice-Admiral Ort, quoted by Nick Brown, *op. cit.*

⁵³ *Ibid*, p. 46.

⁵⁴ *Dutch Submarine Zeeleeuw Completes NATO Counter Piracy Mission*, 5 November 2010, <http://www.manw.nato.int/>

Following an analysis of the media reported actions performed by warships, I came to the conclusion that the task forces can act both in a reactive and active manner.

Reactive posture is given by the military capabilities reaction to a piracy incident. The central idea to prevent piracy in the Gulf of Aden is that if a merchant ship withstands the pirate attack for 30 minutes⁵⁵, by applying the BMP, then it will have created the necessary time for a helicopter to be scrambled from one of the ships engaged in the IRTC patrol. The simple appearance of a warship or a ship borne helicopter will most likely lead to the abandonment of the pirate attack. Thus, a successful military intervention depends to a high degree on the time factor. When pirates get aboard the merchant vessel but do not succeed in taking the crew hostage, due to the fact that the crew locks itself in a safe place, then the conditions are created for the military to storm that vessel in order to release the ship from the pirate control (e.g. Russia – release of the *Moscow University* tanker⁵⁶, the Netherlands – release of the *Taipan* cargo ship⁵⁷, the US – release of the *Magellan Star*⁵⁸). However, if both the vessel and the crew are under pirate control, usually the warships abstain from conducting a hostage release operation given that the crew's safety is at stake. The only exceptions were the US operation (release of the Master of the American flagged *Maersk Alabama* and French operations (*Carre'As* yacht and *Tanit* yacht), the latter concluded with the death of the yacht captain who was caught in crossfire between the French commando and the pirates.

In the spring of 2010, NATO and CMF successfully adopted a new tactic with regard to the already captured ships and used by pirates as mother ships (the so-called *dhow*s). This is characterised by applying a continuous pressure on the pirates with a view to abandoning the captured ship, without escalating the situation⁵⁹, by simply positioning a warship in the vicinity of the hijacked ship.

Proactive posture. Given the detailed intelligence regarding the location of pirate makeshift camps, the most rapid and efficient solution would be the destruction of these camps, thus stopping the *Pirate Action Groups (PAG)* going out to sea where it is much more difficult to be spotted. However, this action

⁵⁵ Massimo Annati, *Non-Lethal Systems for Self-Defence of Merchant Ships*, in *Naval Forces*, no. VI/2009, vol. XXX, p. 45.

⁵⁶ David Williams, *How to Deal with Pirates, Russian-style*, in *Daily Mail*, 06.05.2010, <http://www.dailymail.co.uk/news/worldnews/article-1273818/Russian-commandos-storm-oil-tanker-captured-pirates.html>

⁵⁷ *Dutch Navy Frees German Cargo Ship, Arrests 10 Pirates*, AFP, 05.04.2010, <http://www.france24.com/en/20100405-dutch-navy-frees-german-cargo-ship-arrests-10-pirates>

⁵⁸ *US Marines Capture Ship Hijacked by Pirates off Somalia*, 9 September 2010, <http://www.bbc.co.uk/news/world-africa-11250785>

⁵⁹ *NATO Warship Forces Release of Pirated Dhow*, News Release, 04.04.2010, www.manw.nato.int.

is not possible due to the limited mandate which “*terminates ashore*”⁶⁰, not allowing any action on land. Consequently, starting in March 2010, the TFs (especially those of the EU and NATO) adopted a new posture, much more aggressive, characterised by positioning the warships close to the shore “*applying pressure there where we can, based on the intelligence regarding the activities in the pirate camps*”⁶¹, in order to destroy the pirate boats and prevent them from going out to sea. In order to overwhelm the warships the pirates use the “*swarm tactics by some of the pirates who try to flood the area with action groups*”⁶². In case the pirate boats evade detection, then the airborne means are used to pinpoint them and feed the information back to warships and command centre operations rooms. However, here it appears the so-called “*tyranny of distance*” that frustrated the former EUNAVFOR commander, Admiral Hudson: “*We can have a maritime patrol aircraft (MPA) identify a pirate action group and it can take me two or three days to get a ship down there*”⁶³. Once the pirate mother ships and the skiffs are located by ISR means, these are tracked by the naval capabilities found in the immediate vicinity, in order to be stopped by the ship borne helicopters, which fire warning shots, while the warship closes for intercepting the pirate boats and boarding them with a view to destroying the paraphernalia.

However, there were cases when pirates shot at helicopters, which illustrate the inherent security challenges for helicopter crews. The pirates who succeed in avoiding the ISR location sometimes might be successful in capturing dhows in order to use them as mother ships to operate an extended period of time at extended ranges off the coast.

This proactive approach came out as a result of the Spanish Defence Minister, who summed up the outcome of the EU defence ministers meeting: “*EU flotilla will intensify the pirate ports surveillance and it will hunt down the mother ships*”⁶⁴. Therefore, in the following two months (March-April 2010) from adopting this new tactics, EUNAVFOR disrupted over 40 PAGs⁶⁵.

⁶⁰ *EU Chief Buoyant As New Wave of Somali Pirates Attack*, 05.04.2010, <http://www.eubusiness.com/news-eu/somalia-piracy.3zz>

⁶¹ Richard Scott, *Interview with Rear Adm. Peter Hudson*, in *Jane's Defence Weekly*, 28.04.2010, p. 34.

⁶² Adm Hudson quoted by Nick Childs, *Navies Struggle with “Swarming” Pirates*, 1 April 2010, <http://news.bbc.co.uk/1/hi/world/africa/8598726.stm>

⁶³ *Hi-tech Navies Take on Somalia's Pirates*, in *The Economic Times*, 16 June 2010, <http://economictimes.indiatimes.com/articleshow/6054828.cms?prtpage=1>

⁶⁴ *EU Flotilla Intensifies Control of Pirate Ports*, AP, 25.02.2010.

⁶⁵ *EU NAVFOR French Warship Destroys Pirate Mother Ship*, 29.04.2010, <http://www.eunavfor.eu/2010/04/eu-navfor-french-warship-destroys-pirate-mother-ship/>

Analysing the media articles, I found two situations that reflect the outcome of the confrontation between pirates and the navy ships:

➤ *When suspect pirates are not caught in the act of piracy*⁶⁶, even though they possess pirate paraphernalia, most of the time they are set free, which strengthened the pirate perception that the warships have a weakness. This reflects *“the particularities of the laws of certain states”*⁶⁷, which sends the wrong message, encouraging subsequent pirate actions. Arresting the suspect pirates is a sensitive issue for NATO, as an Alliance spokesperson maintained that NATO TF *“did not have any mandate to arrest and detain pirates, only to disrupt their activities. It was a decision for the commander of each vessel on what to do with captives”*⁶⁸. Looking for a scapegoat, Julian Brazier, the Conservative spokesperson from the British shipping industry, stated: *“The fault lies not with the hard-pressed naval commanders, but the ridiculous rules of engagement (ROE) and operating instructions they are given by their political masters”*⁶⁹. As for EUNAVFOR, *“it restricted its prosecutions of suspects to pirates who were caught in the act rather than those who looked suspicious on the bases of their equipment. This was due to the arrangements for prosecution, generally in Kenya and the Seychelles”*⁷⁰. Thus, at least 200 pirates were freed by EUNAVFOR, in the first four months of 2010⁷¹. Although it might seem unbelievable, sometimes, before being set free, the pirates benefit from medical checks and food aboard the warships⁷².

➤ *When the pirates are caught red-handed*; these are, most of the times retained aboard the warship with a view to being transferred to a competent authority for trial. One of the most delicate issues is the transfer of the pirates to the right

⁶⁶ Usually, when a helicopter turns up, the pirates throw overboard the paraphernalia. However, there are situations when they do not do this, in which case the paraphernalia will be destroyed along with the mother ship (a pirate whaler, but not a ship seized by the pirates) and the attack boats by the warships, only if the pirates have been taken aboard the warship. Usually, when there is no potential for a successful prosecution, the pirates are sent back ashore in one of the skiffs with sufficient fuel and food.

⁶⁷ Roger Middleton, *Pirates and How to Deal with Them*, Africa Programme and International Law Discussion Group, Chatham House, 22 April 2009, p. 4.

⁶⁸ Jon Ungoed-Thomas and Marie Woolf, *Navy Releases Somali Pirates Caught Red-handed*, Sunday Times, 29.11.2009, <http://www.timesonline.co.uk/tol/news/world/africa/article6936318.ece>

⁶⁹ Nick Britten, *Navy Regularly Releases Somali Pirates, Even when Caught in the Act*, 29.11.2009, <http://www.telegraph.co.uk/news/worldnews/piracy/6684210/Navy-regularly-releases-Somali-pirates-even-when-caught-in-the-act.html>

⁷⁰ The European Union Committee of the House of Lords, *Combating Somali Piracy: The EU's Naval Operation Atalanta, Report with Evidence*, 14.04.2010, p. 14, <http://www.publications.parliament.uk/pa/ld200910/ldselect/ldcom/103/103.pdf>

⁷¹ *EU Forces Releasing Hundreds of Pirates in Somalia*, ABC website, 28.04.2010.

⁷² Nick Britten, *op. cit.*

authority for prosecution and for detention when they are found guilty. Basically, this transfer is made in line with the legislation of the warship flag state and also in accordance with a transfer arrangement with an authority from another state that is compliant with the international law regarding human rights. There are states, as Yemen, where pirates run the risk of being sentenced to death⁷³ and this represents a good reason of not handing over the suspects to the Yemeni authorities. In order to have an efficient trial, warships must bring witnesses; strong evidence (paraphernalia, including pictures and video). By 28 April 2010, EUNAVFOR captured and transferred 250 suspects⁷⁴. Based on the reports issued by mass media, I have identified a series of options for the transfer of suspect pirates that have been adopted by the warships:

- *Option of transferring the suspect pirates to the Somali authorities* (especially those in Puntland) would be the normal protocol, which reads that the state from where the pirates originate is responsible for their trial. This option is limited by various factors (possible complicity of the authorities, non-compliance with the human rights law during the trial, standards of living in the prison). However, France handed over to the Puntland authorities the suspect pirates captured by its warships⁷⁵.
- *Option of prosecuting the suspect pirates and imprisoning them in the state that arrested them* entails that the state bears all the costs. On top of this, there is apprehension with regards to the fact that these pirates will benefit from getting the political asylum status upon completing their prison sentence, since they might be tortured or executed in Somalia. Nevertheless, there are nations that opted for this solution (the USA and France).
- *Option of transferring the suspected pirates to the authorities belonging to the flag of the attacked merchant vessel.* This was used by the USA (an attacked Omani vessel) and the Netherlands (an attacked German vessel).

In order to overcome the problems incurred by the above-mentioned options, some nations resorted to *prosecuting the suspect pirates in a third party state in the region and setting up a specialised international tribunal*. This is used intensively by EUNAVFOR (following the agreements signed by the EU with Kenya and the Seychelles), as well as by the USA and UK. This entailed adapting the third state party juridical system (prosecution, trial process, detention)

⁷³ *Yemen Sentences Somali Pirates to Death*, 18.05.2010, http://news.bbc.co.uk/1/hi/world/middle_east/8689129.stm

⁷⁴ *EU Forces Releasing Hundreds of Pirates in Somalia*, ABC website, 28.04.2010.

⁷⁵ *French Navy Hands Over Suspected Pirates to Somalia*, 13 March 2010, Reuters.

to the international standards regarding the human rights law, aspects which have been dealt with by *UNODC (UN Office of Drugs and Crime)*. However, the capacity of these countries to process a high number of suspect pirates is limited. Consequently, the overburdened Kenyan juridical system and the unfulfilled commitments of the EU to deliver assistance in the juridical sector led Kenya to announce revoking the agreements with the EU in the spring of 2010. Eventually, the EU had to start diplomatic talks with Kenya and offered concrete solutions to support it. In order to ease the burden on Kenya, in May 2010, the EU signed an agreement with Tanzania. It has also been taken into account an agreement with Mauritius, Mozambique, South Africa and Uganda⁷⁶.

There is another option that is pursued by some nations: *setting up an anti-piracy international tribunal*. This is a Dutch-Russian project, started with a view to solving the judicial issues. Consequently, as a permanent member of the UN Security Council, Russia initiated the draft regarding a resolution to set up a specialised court that was approved by the UNSC members, 27 May 2010⁷⁷. The same resolution requested the UN Secretary-General (UNSG) to present a report regarding the possible options for prosecution and detention. Consequently, on 23 July 2010, the UNSG presented his recommendations, suggesting seven options⁷⁸ that ranged from less specific to concrete solutions among which the establishment of an international tribunal by Council Resolution stood out. Moreover, on 25 August 2010 the UNSG announced the appointment of a special adviser on legal issues related to piracy off the coast of Somalia.

*

Somali piracy has the tendency to extend almost to the entire Indian Ocean surface, given the longer range of attacks. This development could be seen as an adaptation of the pirates to the pressure applied by warships and as an exploitation of the OPSEC deficiencies in both the civilian and military domains.

Counter-piracy achieved through the deployment of warships with a view to protecting shipping and disrupting pirate actions has led to an unprecedented coordination of navies, which can develop into a unique situation in which *“towards the end of 2010, the US warships could be coordinated by a Chinese admiral”*⁷⁹.

⁷⁶ http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/113482.pdf

⁷⁷ *Netherlands and Russia to Jointly Explore Piracy Tribunal*, <http://www.netherlandsmission.org/article.asp?articleref=AR00000693EN> and *EU, NATO Warships Destroy Three Mother Ships of Somali Pirates*, ITAR-TASS, 02.05.2010, <http://www.itar-tass.com/eng/level2.html?NewsID=15086755&PageNum=0>

⁷⁸ Report of the Secretary-General on possible options to further the aim of prosecuting and imprisoning persons responsible for acts of piracy and armed robbery at sea off the coast of Somalia, 26 July 2010, <http://www.securitycouncilreport.org/atf/cf/%7B65BF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/Somalia%20S2010%20394.pdf>

⁷⁹ Statement of Commodore Hans Christian Helseth, former DCOS OPS MC Northwood, in the paper signed by Gwladys Fouche, *Rising Piracy May Prompt More Joint Naval Action – NATO*, Reuters, 12 March 2010.

At the same time, this framework offered China and Japan the chance to play a more important role in the naval arena, both having ambitious projects of establishing naval bases in the Horn of Africa. Moreover, the counter-piracy operations, even though characterised by numerous challenges, most of them of a political nature (juridical dilemma, ROE), test to the maximum the readiness of the crew in high tempo MSO. The downsides are the large number of capabilities necessary to cover the area and the huge costs incurred by sustaining the warships (e.g. a six-month deployment of a Norwegian frigate costs 30,7 million USD, being the equivalent of paying 100 000 Puntland police officers for the same period of time⁸⁰). As for the risks to which the warships are exposed, we have seen that the warships have come under direct attack from pirates. Moreover, the ships are operating in an area (Gulf of Aden) which is notorious for the occurrence of maritime terrorist attacks.

The fight against piracy has led to the division of work between the western nations and the regional states. The former have committed to send naval capabilities, whereas the latter have contributed their own juridical institutions (tribunals, prisons), which has already appeared to show signs of *“fatigue”* (e.g. Kenya). It can be affirmed that the fight against piracy has contributed to the reform of the juridical systems of the regional states that have accepted to prosecute, put on trial and imprison the pirates. Punishing the pirates, regardless of the authorities that take this decision, would act as a deterrent for pirates. Against this background, a decision to set up an anti-piracy international tribunal would give a new impetus to the judicial sector. In addition, putting into practice the regional initiatives (e.g. *Arab Task Force*) might lead to a situation, although less probable, where the regional navies take over from the international navies the responsibility of combating piracy.

The success against pirates has not taken shape yet, in spite of a dip in the number of the attacks (164) in the first 10 months of 2010, compared to (193) the same period of the last year⁸¹. On the contrary, it can be inferred that there has been an increase in the pirate efficiency in the context of a smaller number of attacks conducted by pirates that seized 37 ships this year compared to 33 ships last year⁸². Nevertheless, the decline in pirate attacks can be attributed to the new proactive tactics adopted by the Task Forces, which resulted in the destruction of the pirate paraphernalia leading to diminishing their material resources

⁸⁰ Stig Jarle Hansen, *Piracy in the Greater Gulf of Aden*, *op. cit.*, p. 30.

⁸¹ *Somalia Pirates Increase Hijackings: UN*, AFP, 2 Nov. 2010.

Worldwide Hijackings Rise as Pirates Expand Area of Operation, 21.04.2010, http://www.icc-ccs.org/index.php?option=com_content&view=article&id=406:worldwide-hijackings-rise-as-pirates-expand-area-of-operation&catid=60:news&Itemid=51

⁸² *Ibid.*

and hampering the regrouping of pirates to execute other attacks. In this context, the role of the security teams on board the merchant and fishing ships should not be underestimated by the shipping/fishing industry, having in mind the deterring effect produced by the simple presence of the security team. The protection measures taken by the merchant ships have led to the development of new profitable markets, not only for the manufacturers of non-lethal weapons but also for the private security companies.

The international maritime approach is necessary, albeit it does not offer a long-lasting solution since it is a reactive response that focuses on limiting the phenomenon. This has been the fastest and the handiest solution for the international community and it can be seen as an intermediate option as well as a complementary one to an international initiative ashore aimed at eliminating piracy roots. This should consist of a package focused on the reform of the Somali security sector and the development programmes.

Bibliographical References

- Best Management Practices 3, *Piracy off the Coast of Somalia and Arabian Sea Area*, June 2010, Witherby Seamanship International Ltd, www.britanniapandi.com/download.cfm?docid=8838B55F-72DC-4D97-BF2841A5865A7DAF
- Joseph George, *Naval Presence Cuts Regional Piracy by Half*, 22.03.2010, <http://www.business24-7.ae>
- Andrew Langley, *100 Facts on Pirates*, Bardfield Press, 2006.
- Gheorghe Marin, Andrian-Sirojea Mihei, *Terorismul maritim. Mît și realitate*, Editura Centrului Tehnic-Editorial al Armatei, București, 2010.
- Laurențiu Meșterca, *Modern Maritime Piracy – A New Risk to Security in the 21st Century*, in *Romanian Military Thinking*, no. 1, 2010, pp. 81- 94.
- Michael Scott Moore, *How Do You Prosecute a Pirate ?*, www.miller-mccune.com
- Richard Platt, *Pirate*, Eyewitness Guides, Dorling Kindersley.
- *UN Office on Drugs and Crime (UNDOC), Counter Piracy Programme*, November 2009, http://www.unodc.org/documents/easternafrika//piracy/UNODC_Counter_Piracy_Programme.pdf
- UN Security Council Resolutions with Regard to Somalia no. *1772/2007, 1814/2008, 1816/2008, 1838/2008, 1928/2010*.
- Lee Willet, *An "Awakening" at Sea ? NATO and Maritime Security*, RUSI, <http://www.rusi.org/go.php?structureID=commentary&ref=C49DB11644DE78>
- *UNCLOS*, http://www.un.org/Depts/los/convention_agreements/convention_overview_convention.htm
- http://www.shipping.nato.int/NATOShippi0/Newsletter/file/_WFS/Newsletter%20April%202010a.pdf
- <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA522959&Location=U2&doc=GetTRDoc.pdf>
- Sites of EUNAVFOR: www.eunavfor.eu, MC Northwood: www.manw.nato.int and TF 151: www.cusnc.navy.mil/cmfi/151/index.html

SECURITY CHALLENGES VIA THE INTERNET

Dr Petre DUȚU

The security environment currently faces a series of challenges (security dangers, risks and threats). Among them, a central place belongs to: international terrorism; proliferation of weapons of mass destruction; frozen conflicts; organised crime. At present, security challenges coming from the virtual environment via the Internet add to these: cyberterrorism; cybercrime; hackers' actions. Consequently, the current security environment comprises both the real and virtual environment.

Thus, the author points out that, when we refer to the security environment, one must concomitantly take into account both environments, which are in a continuous and constant interdependance and interaction.

Keywords: *cybercrime; cyberterrorism; security challenges; cyberspace; security environment*

Security environment faces a series of challenges that are rooted in both real and virtual environments.

Dangers, risks and threats to security in the cyberspace usually come via the Internet. To properly understand the “*route*” of security challenges, we will define the terms *cyberspace*, *real environment*, *virtual reality* and *security environment*.

Terminology explanations

Cyberspace is a word coined by the American writer William Gibson¹. The original meaning of the term “*cyber*”, deriving from the Greek “*Kubernao*” or “*Kybernetes*”, is the verb *to lead* and also represents the root of the term “*to govern*”². The semantic connotation evokes, on the one hand, the idea of navigating through electronic data and, on the other hand, the possibility to lead,

due to the control over these data.

The cyberspace of William Gibson is not a passive data universe like a library. On the contrary, it provides communication channels between this data world and the world called “*real*”. Indeed, so far, the Internet user has visited a website, selected the information of interest and then loaded it on the personal computer. This is called the *pull* method. However, through the new generation of browsers,

Colonel (r.) Dr Petre Duțu, Senior Researcher, the Centre for Defence and Security Strategic Studies within “*Carol I*” National Defence University.

¹ Cf. J. A. Graham, *L'Internet est un nouvel espace international au sens du droit international public*, http://www.alfa-redi.org/gic/cyberspace_thesis.pdf, p. 3.

² *Ibidem*, p. 4.

it is possible to select sites that will automatically send the information to the PC³, at regular intervals, when one speaks of the *push method*. Thus, it is possible to receive the newspaper, television programmes or email – that one no longer needs to search.

As far as the word “*space*” is concerned, it simultaneously recalls more ideas. Firstly, the scope, whose content cannot be grasped at once – which perfectly corresponds to the fundamental nature of a network that connects a limitless number of other networks. Secondly, space allows freedom of movement between different places – which is the very idea of the TCP/IP⁴ that allows information to circulate to and from different PCs, no matter the physical place they may be placed in. Thirdly, space involves geometrical concepts such as distance, direction and dimension. This idea appears in the virtual reality techniques that involve creating three-dimensional PC environments that interact once they are manipulated by the user⁵.

Relationship real environment – virtual environment. There is a *real environment* and a *virtual environment*. *The first* is a physical, concrete, material one, in which people live their lives in the multitude of their dimensions and complexity and perform their professional, cultural, military, political, social, diplomatic, economic activity. This environment is differently and diversely represented by people, as individuals, by local and national communities. *The second* environment adds to the first one, being a result of the technological progress, especially in the field of information and communications. Apparently, it is immaterial and difficult to be exactly localised. For example, an email to a person who has an email address that can be accessed from any PC anywhere in the world on condition it is connected to the Internet. However, this type of environment is “*real*” enough to act itself, of course electronically. It seems that everything that “*happens*” virtually is, to some extent and in a certain way, related to the real environment. Firstly, any action in the virtual environment is carried out, at least initially, from the real, concrete, environment. Then, all the changes, transformations and/or mutations occurred in the virtual world are reflected, in one way or another, in the real world. In other words, they have a bearing on the facts and on the way the person who acts in the virtual environment behaves, thinks and acts.

In our opinion, even video games with different topics are reflected in real life. Thus, the life of a child, young or adult person who spends the majority of time performing different PC activities is affected in one way or another. It is possible for that person to experience a strong sense of satisfaction and fulfilment individually,

³ PC = personal computer (A. N.)

⁴ Transmission Control Protocol/Internet Protocol, <http://www.alexandrupacuraru.ro/?p=349>.

⁵ Michael Heim, *The Metaphysics of Virtual Reality*, London, Oxford University Press, 1993, p. 82.

but to be socially isolated or detached from everyday reality. At the same time, cyberspace allows individuals who access it to create their own world that may sometimes be totally different from the real one.

In addition, cyberspace is “full” of information provided not only by the human society, which uses it for different purposes and objectives, but also by those who create their own virtual world. The veracity of this information cannot be guaranteed by anyone. The source of the data in the virtual world may be often missing or hidden. Moreover, it is relatively free for any person to access the cyberspace. Each Internet user leaves its mark in the cyberspace. In turn, the latter influences the opinions, attitudes and behaviour of those who access it. Therefore, we can speak about interdependence and inter-conditioning between the two environments – the virtual and the concrete, physical one.

Virtual reality. Lexically, the term “*virtual reality*” is an oxymoron, i.e. a figure of speech that consists in forming an expression that puts close two terms that have *a priori* opposite meanings. In the applicative field, the “*virtual reality*” domain has its source in the one of simulation, in which a computer reproduces, in real time and in an as accurate as possible manner, a real, physical model. Such systems are the ones designed for learning to pilot a plane or, more currently, video games, seeking maximum realism.

Virtual reality helps people to enter an artificial world. This world can simulate real world conditions or create a new world conditions. The human and virtual world interacts, which is translated for humans into putting in practice the quasi-totality of cognitive faculties: perception, action, memory, emotion, motivation. These are natural abilities, but they are used in new contexts. Thus, they must be combined with the virtual world. Relying on virtual reality applications, we proceed to a study of the cognitive faculties put in practice and their adaptation.

With regard to the *real/reality* duality, we appreciate that *reality* is what we perceive from the real. On the other hand, the term *virtual* does not fully cover the virtual in its aggregate. It is limited to the context of *virtual reality*. Moreover, in the field of information technology, there is confusion between different qualifiers such as: virtual, electronic, digital, artificial, synthetic, all of them defining an artefact produced by the machine (as opposed to human, natural, physical, real).

Security environment. It designates a reality represented by the system of favourable conditions, domestic and international, ecological, social, economic, military, diplomatic, political, informational and cultural in which any human community exists and performs its activity. It represents the space (place) where the state of security/insecurity gets manifest at the individual, group, state level

as well as at the zonal, regional and global one. The security environment has a complex structure and its evolution depends on a multitude of national, regional and international factors⁶.

If we consider the virtual environment existence and manifestation and its significant relationship with the real environment, then we can say that the security environment has to “cover” both. In other words, now, when we refer to the security environment, we have to concomitantly take into account both environments – real and virtual –, which are in a continuous and constant interdependence and interaction.

The Internet as the place and form of manifestation of the virtual

The proper name *Internet* refers to the *World Wide Web*, the single global network of computers interconnected through the communication protocols *Transmission Control Protocol* and *Internet Protocol (TCP/IP)*. The precursor of the Internet dates back in 1965, when the *Defence Advanced Research Projects Agency* of the US Department of Defense created the first network of interconnected computers called *ARPAnet*. The super-network of nowadays is the result of the *ARPAnet* extension. The common noun *Internet* designates, in most cases, the same network, seen as a means of mass communication, together with the information and services that are offered to users via this medium. Technically, the term may also designate a network that interconnects two or more independent networks located far away from each other. Examples of large networks that justify the use of this name are *SIPRNet* and *FidoNet*.

In a certain way and to a certain extent, the Internet can be considered the place and the form of manifestation of the virtual environment. In support of this assertion, we start from the fact that the Internet, taking into account the way it appeared, is an environment (of course, a virtual one) where, through information, people “meet”, communicate and perform many other activities.

In our opinion, the Internet, as the virtual environment form of manifestation, distinguishes mainly through the concept of *virtual community*. It⁷ refers to people reunited *via* the Internet by common values or interests (e.g. a hobby, leisure time or profession). The community goal is to create value based on exchanges between members, for example, sharing advice and debating issues. To put in practice a virtual community may be beneficial for a website, because it creates

⁶ Petre Duțu, *Mediul de securitate în contextul globalizării și al integrării regionale*, Universitatea Națională de Apărare, București, 2007, pp. 83-120.

⁷ Communautés virtuelles, <http://www.commentcamarche.net/contents/web/communautes-virtuelles.php3>, p. 1.

a sense of belonging to a particular group of people and allows the site to evolve into a participatory approach. In addition, a community of users that has a considerable size may be valued for the image of the site, as it provides a strong sympathy capital and creates a feeling of confidence for the Internet user. However, if the perimeter of the community is not correctly defined, splits and frustrations may appear. Then, the community risks not producing the intended effect, but the opposite one, namely to convey a negative image.

In time, the Internet has begun to broaden the range of activities it facilitates. Although in the beginning, electronic games were those that occupied more time and space, today, a series of public services solve a major part of their tasks via the Internet. Broadly, the virtual community will include all those who use the facilities offered by the Internet, from electronic games to a source of information of great diversity – from the railway timetable to bibliographies and texts for almost all professions. Hence, the need for regulating, from a legal perspective, the “*virtual community*”, namely the virtual environment occupied by the Internet. However, the multitude of communities does not constitute an obstacle to the existence of a large unifying community: the virtual community. Its most obvious proof is the establishment of a new discussion group in *Usenet*⁸. To create it, one must have, on the one hand, the approval of a certain number of groups that already exist and, on the other hand, the implicit acceptance of those who administrate the servers of the groups, most often access providers and universities. Indeed, if the latter ones do not approve this new group, the Internet users that have subscribed to their service cannot have access to the messages of the new group. The approval or refusal of a discussion forum meets, in general, the common criteria for all virtual communities: values such as respect for freedom and democracy, attitudes such as anti-racism or the standards of conduct that prohibit advertising in *Usenet*.

It is clear that the real and virtual world will increasingly merge: “*The exponential growth of information, the development of social networks and the accelerated increase in the video traffic will progressively cause an interconnection between the virtual world and the real world*”⁹. These represent implications for humanity and the Internet.

Along with the Internet, global society becomes, each year, more and more complex and interdependent. Governments, multilateral organisations, the private sector and the civil society now recognise that they are often powerless when they act individually: global problems, threats, opportunities and challenges they have to cope with often go beyond the individual capacity, no matter how powerful each of them may be.

⁸ Roland Trique, *Le jargon français*, <http://www.freescape.eu.org/eclat/lexique.html>

⁹ Rod Beckstrom, *Le futur de l'ICANN*, <http://www.icann.org/fr/presentations/future-of-icann-beckstrom-28jan10-fr.htm>, p. 2.

We increasingly notice the influence and potential of the Internet in various fields of human activity at local, national, regional and global level. Science and innovation that develop by means of the web have to face these challenges when the universal arteries of the Internet cause developments and stimulate economies.

Security challenges *via* the Internet to the security environment

As the Internet becomes increasingly ubiquitous in various fields of human activity, individuals or groups can resort to the anonymity offered by the cyberspace to threaten the citizens of different communities and countries on the grounds of ethnic background or religious and political beliefs. They can do it without the risk of being captured, wounded or killed, as if in the event of a similar act in the real world. As the Internet grows increasingly extending at both national and world level, cyber terrorism acts can multiply. Computer systems, the favourite target of cyber terrorists, will continue to be affected by sabotage or terrorism *via* cyberspace. Besides it, both independent individuals and organised groups commit illicit and illegal acts on the Internet. They are the authors of what is called cyber crime. *Cyber crime* or *computer crime* describes the exploitation of the information and communication networks without any constraint related to geography or data movement. Cyber criminals are, however, less anxious than the delinquents that operate in a traditional manner, as deviant behaviour occurred on the Internet is not criminally sanctioned in many states. Hence, there is a need for legal regulation of the activities in the cyberspace at both national and international level. Even the nature of the Internet requires an effort to secure networks beyond the traditional state boundaries.

All these acts, which fall into the category of computer crime, affect human security, nationally and internationally. Therefore, the legal terminology has to assimilate these new security challenges. They affect the intellectual property, privacy, databases and other inappropriate uses (i.e. illegal and illicit) of the information about individuals, institutions, companies, and other entities. Thus, through the Internet, it is possible not only to steal or alter data and data processing systems, but also to borrow an identity or an authorisation and to use them for illicit operations, from distance and in anonymity.

Currently, we discover that information has three offensive uses¹⁰, as follows:

- an unwanted adjustment, the price of its sustainability. No matter what the information related to things may be (techniques that authorise certain performance, knowledge that determines strategies) or to people (location, registering, monitoring and accountability), they are power

generators. With the loss of protective privacy, ranging from the theft of license to the invasion of privacy, there is always the danger and loss for someone; practically information threatens privacy;

- a harmful penetration, price of its transmissibility, is also an acting force. It creates and destroys things or relationships; it produces from order to disorder. In particular, the false, destructive and occult information related to the truth affects the ability to act in an appropriate manner, destroys memory and annihilates the processing capacity. From political misinformation to computer viruses, from falsehood to sabotage, information threatens information;
- an unacceptable spread, the price of its responsibility. The monopoly on making it public or the control on its reception, through manipulation or propaganda, threatens critical thinking, the possibility to respond, and significantly damages any free human relationship. This way, information threatens communication.

Practically, the Internet uses information as a raw material for all its activities. Hence, its social, economic, political, cultural importance, as well as its vulnerability to various and diverse challenges. Among them, an important place is held by the activity of hackers. They are young people who are experts in computer science and who sometimes succeed in entering illicitly in the computers of institutions or companies. Perhaps there are thousands of hackers today, and several hundred of them are able to penetrate computer systems no matter how sophisticated they may be¹¹.

Hackers maintain an ambivalent relationship with the secret. Being illegal, their work involves anonymity, but the need to be recognised within the community of hackers presupposes for the committed piracy to be widely known. According to a study conducted by the Computer Security Institute, more than 40% of companies have found at least one invasion attempt in 2000¹². Pirated servers, stolen bank card numbers, disfigured websites: pirates on the Net make people speak about them more and more. However, the objectives and details of their actions remain unknown. Most hackers state they enter the computer systems because of their passion for computer science and not because of other reasons. It seems that the pirates who attack servers to earn money or to access financial data are not too many. However, any hacker attack may affect the existing data in the system that has been hacked. Hence, there is a need to protect computer systems against hackers.

¹⁰ François-Bernard Huyghe, *Violence dans la société de l'information*, http://www.strategic-road.com/intellig/infostrategie/pub/violence_societe_information_txt.htm, pp. 3-4.

¹¹ *Qui sont les hackers ?*, http://www.scienceshumaines.com/-0aqui-sont-les-hackers-0a_fr_10628.html

¹² See Burçin Gerçek, *Piratage informatique: ce que veulent les «hackers»*, <http://www.symantec.com/region/fr/resources/pirate2.html>

Along with cyber crime and hackers activity, cyber terrorism is a security challenge that is important as well as urgent. Moreover, after 11 September 2001, highly computerised countries began to consider seriously the threats related to cyber terrorism to their companies and the society, in general.

Cyber terrorism is the convergence between traditional terrorism and networks, starting with the Internet. Therefore, cyber terrorism can be defined as the deliberate action meant to destroy, degrade or alter data, information flows and vital computer systems belonging to states or companies that have strategic value for the proper functioning of a country, in order to cause damage and/or to slow down the activity at the maximum, because of political, religious or ideological reasons. These damages may be economic, social, environmental and even vital to individuals, in certain cases. A distinction between cyber terrorism and simple cyber crime should be made, as the latter consists in using a system for an illicit purpose. Similarly, cyber terrorism should not be mixed with hacker activity that is sometimes motivated by ideological elements too, but especially seeks to disrupt the functioning of public institutions and other organisations.

Cyber terrorism is successful for at least the following reasons¹³: 1) the cost of access is low – a laptop is less expensive than a high explosive or a combat weapon and there is no risk to draw the attention of the state institutions with responsibilities related to weapons and munitions; 2) once our societies become more and more dependent on information networks, their disappearance may cause considerable economic, logistical and emotional effects. In addition, the public and journalists are fascinated with all the types of computer attacks, which leads to a wide media coverage; 3) the developed countries paralysis when they are deprived of their computer networks. It is, in part, one of the objectives pursued by international terrorist groups.

The target of cyber attacks will particularly be the following: telecommunication management facilities (telephone stations, GSM access points, spinning and non-spinning networks, and satellite and hertz relays) for energy generation and distribution sites (nuclear, thermal plants); transport coordination facilities (airports, ports, maritime and air traffic control, railway stations, highways, crossroads regulating systems in large conurbations), petroleum products distribution facilities (refineries, storage networks of service stations), postal business management centers, water distribution sites (treatment plants, analysis centers, purifying plants), financial and banking institutions (national stock exchanges, ticket distribution networks); emergency services, health and public security (police, fire departments, hospitals, the systems of intervention in case of emergency), government services (social security, medical insurance and institutional sites), media (television chains,

¹³ See Patrick Chambet, *Le cyber-terrorisme*, <http://www.chambet.com/publications/Cyberterrorisme.pdf>

press groups), symbolic elements of society and lifestyles (large distribution, industry representatives).

Therefore, a simultaneous attack on multiple targets would be devastating for a country unprepared to cope with such an attack.

*

The development of information and communication technologies has enabled the emergence and widespread manifestation of the virtual environment. The Internet is one of the most significant ways to use cyberspace.

From a sociological standpoint, “*virtual*” is a variable of the security environment spatial dimension. It is due to at least the following reasons: through its characteristics, virtual reality is a continuation of the real dimension without being a copy of it; virtual environment has become one where a large variety of concrete human activities are carried out; the existence and manifestation of certain security challenges in the virtual environment that may affect the security environment; the continuity of the virtual and real environment in terms of human activity.

The real and virtual environments interact and overlap. They communicate constantly. The Internet, through the multitude of functions performed, contributes to the achievement of such communication. In addition to the social, cultural, economic etc. facilities, the Internet can “*host*” less legitimate activities. Thus, a number of security challenges – dangers, risks and threats – come from the Internet, namely from the virtual environment to the real environment. They mainly refer to cybercrime, cyber terrorism and hacker activity.

Therefore, legal regulation related to the Internet activity is needed both at national and global level. This shall be taken into consideration with a view to conjugating the activities meant to prevent and combat the security challenges generated in the cyberspace and electronically “*sent*” to the real environment where their damaging effects become noticeable.

Selective Bibliography

- Gilles Deleuze, *Différence et Répétition*, <http://www.protevi.com/john/DG/DR.pdf>.
- Marcello Vitali Rosati, *La virtualité d'Internet*, <http://www.sens-public.org/spip.php?article669>
- <http://ro.wikipedia.org/wiki/Internet>
- <http://www.symantec.com/region/fr/resources/pirate2.html>
- *Qu'est-ce que la virtualisation ?*, <http://hypermedia.univ-paris8.fr/pierre/virtuel/virt1.htm>

English version by
✍️ *Diana Cristiana LUPU*

TENDENCIES IN THE EVOLUTION OF LOGISTIC SUPPORT IN FUTURE CONFLICTS

Colonel BEng Teodor INCICAŞ

NATO and its member states are on the edge of a new transformation generated by the already configured New Strategic Concept, as well as due to the engagement in the challenging operations of this millennium, such as ISAF. Based on some hypotheses, such as: NATO will stay more than 10 years in Afghanistan or the models launched by the operations in Iraq or Afghanistan cannot be universal etc., we can draw the main tendencies regarding the evolutions in the area of the logistic support for the future conflicts, envisaging the next 10-15 years. These directions mainly refer to a more efficient logistic support, based on more flexible forces (deployable, predictive, adaptive and responsive), a suitable relation military/contractor, and a new philosophy in so far as the costs are concerned.

Keywords: *logistics; logistics system; multinationality; costs; logistic support*

Modern armed confrontations and, implicitly, military operations, in particular, bear the mark

of the current period – the information age –, of the economic and technological evolutions, as well as of the social or geopolitical turmoil, in which ethnic and religious contradictions and misunderstandings are bigger and bigger, up to military conflicts.

At the same time with the exacerbation of terrorism and the outbreak of antiterrorist war at the world level, the asymmetrical confrontation is more and more important in the military conflicts nowadays. Therefore, flexibility, rapid deployment and forces manoeuvrability in the most terrible conditions and at long distances from the national territory represent prerequisites alliances and states should consider regarding the large units and units that act in the joint multinational operations at the beginning of this century.

On the other hand, as far as NATO is concerned, currently, the organisation is on the brink of a new evolution, given the *new strategic concept*, through which it tries to define its role and its fundamental

Colonel BEng Teodor Incicaş – Chief of Staff at the Joint Logistics Command.

missions at the beginning of this millennium. Moreover, it is engaged in the *ISAF* operation in Afghanistan, which arouses considerable political, moral, military and material attitudes.

In our opinion, these efforts cannot be accomplished, orientated and exploited without the existence of some general or specialised bodies of the Alliance whose systemic quality actions become force multipliers.

Considering the presented facts, there are certain conclusions that can be drawn, which will lead us to some considerations, we believe, edifying, regarding the logistics of future conflicts. They are aimed at opinions based on own observations and analyses and take into account the attitudes of specialists in the field, grounded especially on the lessons learned following the conflicts in Iraq and Afghanistan. That is why we reckon there are certain hypotheses and statements that subjectivate the identified tendencies, as follows:

- the time horizon considered is of 10-15 years;
- it is possible for NATO not to withdraw from Afghanistan in the following ten years, which outlines the hypothesis that ISAF will remain the major operation of the Alliance in the next decade;
- the models based on the operations in Iraq and Afghanistan are not and cannot be universally applicable, but they are highly important, because they cause changes at the projection and structuring level in the logistic field;
- in the next period, essential, unforeseen changes might occur, following the evolution of technology, in conducting operations and, implicitly, in the logistic field;
- in the next 5-10 years, the Romanian Armed Forces will be provided with effective logistic technique; otherwise, the tendencies for development in the field of logistics in NATO will remain simple models for the national forces.

In this context, in our opinion, the main tendencies that will manifest in the logistic support of future operations will include:

◆ *The increase of multinationality in the logistic support of forces*

The accomplishment of a support effort of common level for the multinational combat units can be made only with logistic structures put together based on the same principle. Currently, only a few logistic systems of allied states can generate their own support, capable of sustaining the forces deployed at big distances from the national territory for several years. The other nations will seek to team up in order to form multinational logistic units. Currently, many of these countries negotiate bilateral agreements with the states that are most important in terms

of logistic potential, yet, in the future, as own needs increase, such states will no longer want such partnerships.

As a consequence, we believe that in the future we will witness the appearance of several integrated multinational logistic units, which will be established especially in the field of *Reception, Staging & Onward Movement – RSOM*, as well as in that of forces support, including transport of materials, supply and, especially, infrastructure engineering for logistics. Most probably, maintenance will not favour the same opportunities, because of the lack of technical compatibility between allies, generated by the still big differences regarding equipment.

From the point of view of the modes of multinational logistic support, as presented in *AJP 4.9*¹, we anticipate the following evolutions:

- Host Nation Support – HNS remains a basic approach, adapted for Article 5 operations, conducted on NATO territories; the latest conflicts (Iraq, Afghanistan) have proved that, in order to realistically plan such operations, it is fairer not to rely on HNS, in any of its dimensions; besides, if we carefully analyse the requirements of Force Goals (even of the partnership objectives), we will notice that the units are required to be capable of acting in areas in which the HNS is reduced;
- lead nation – a mode of support which is still in force, but with certain limitations, considering the few states capable of such a status; it will manifest especially in support of the forces that act in a large multinational unit, whose lead nation can assume the same role at the level of forces support;
- role specialist nation – the cost control for certain strategic resources at the level of the theatre of operations will determine that this option will be always considered when referring to oil supply, local transport services or services related to operations within RSOM (port services, transport to station areas, supply in station areas etc.);
- bilateral agreements – their volume, as shown above, will decrease; yet, they will remain in force in countries engaged in strategic partnerships, as well as when it will be accepted that some states increase their effort in terms of combat structures, as compensation for the logistic support provided;
- the use of alliance/coalition specialised organisations – in the future, the increase in the role of *NATO Maintenance and Supply Agency (NAMSA)* in allied operations will become a certainty; it should become in charge of the mission of specialised structure in the procurement of local services

¹ Source: *AJP – 4.9, Modes of Multinational Logistics Support*, NATO, 2005.

to the benefit of forces; moreover, it will be capable of facilitating the maintenance effort for the common pieces of equipment for which the Agency develops, since peacetime, armament partnerships; in our opinion, *NAMSA* could become, in the ensemble of multinational organisations, the most important support element in the third line.

◆ *The increase in common financial support for covering logistics costs*

Approaching a new vision in relation to covering the logistic support expenditure in NATO operations (even as far as NATO-led operations are concerned) can generate an increase in the quality of logistic support for the forces deployed at strategic distances from the allied territory, in parallel with easing national efforts. At the same time, we believe that such an approach will lead to the increase in the multinationality in logistic support. However, as a negative tendency, we will witness the reduction of national interests in forming own logistic structures necessary for achieving self-sustainability at all levels of military operations.

◆ *A new balance in motion in the military-civil equation in forces support*

We define *balance in motion* as being *that stable state obtained through a succession of successive sub-states, in which the relations between the components of an ensemble (not necessarily a systemic one) may vary depending on the evolutions of the external environment, so that the main characteristic remains in the pre-established fundamental graphic state/repartition*. In the current case, the military-contractor balance in support of allied operations will evolve considering the cost of the product/service, as a dominant characteristic. It will be determined by the following variables: the intensity of the armed conflict; the location and distance from the theatre of operations; the characteristics of the theatre of operations.

◆ *The increase in the fluidity of logistic support*

In our opinion, this tendency will manifest through:

- the accomplishment of an efficient management of the logistic supply chain; in this respect, the Alliance has already been experimenting, for the theatre in Afghanistan, the concept of *Operational Logistic Chain Management (OLCM)*; the implementation of this concept will depend on both the will of nations to invest funds in effectively putting it into practice and the acceptance, by some member states, of the coordination of the logistic effort, on the whole, by NATO bodies;
- the achievement of total visibility on the movement of goods from/towards the theatre of operations; even if the implementation of this concept is unitarily accepted by the allied states, we believe that it depends, however, on the national financial resources and the way in which nations will understand the need for such own systems (which are firstly aimed

at monitoring the movement on the national territory); by extension, full success will belong to the countries that develop their own logistic information systems, which also includes the function of tracking transports and goods;

- the unique control of transports inside the theatre of operations, especially air ones.

◆ *The increase in the joint character of logistic support*

Accomplishing an actual, efficient and effective logistic support cannot take place without a complete jointness and combination of the logistic effort. Thus, the use of logistics components from more armed services is unwise if the effort is not combined, but made in parallel. In order to do that, a modular structuring of logistic forces will be sought, either through an organisation chart that is specific to this desideratum or through the creation, at the level of logistic large units and units, of the capacity to generate certain modules that are capable of joining in support groups. We believe that such a jointness of the logistic effort, doubled by the interoperability in the field, will also manifest at the level of the multinational logistic support. To conclude, we state that, from a certain level of the sustained forces, the logistic support with type-units will be replaced by the use of support groups.

◆ *Logistic forces will become more predictive, adaptive and responsive*

In future conflicts, logistic information, respectively obtaining and processing it, will play an important part. Logistic support forces must be capable of adapting their effort to the dimension of the supported structures, as well as to the type of operations conducted. The conflicts at the beginning of this century have shown that joint multinational operations, from the point of view of the conflict's typology, represent a mix of combat, support and reconstruction actions, sometimes taking place at the same time. On the other hand, information mastery is the key to predictive logistics. From this perspective, the logistics of the future is bound to be the one of optimal stocks. No logistic system can afford the supplementary costs needed for a surplus of stocks. At the same time, building undersized stocks leads to assuming increased risks and that is why the optimum must be reached based on a realistic evaluation.

The responsiveness of logistic forces will depend not only on mastering and correctly processing logistic information, but also on the technical level of logistic equipment, especially the one necessary for the handling of materials and for transportation. In the areas of joint operations, this concept will mean the verticalisation of support. There will no longer be conceptual limitations in this respect. Therefore, the transport battalion of the logistic base/brigade will transport materials, more and more often, to the department of the infantry company.

◆ *The increase in the costs of forces logistic support*

In keeping with the data of the Stockholm International Peace Research Institute – SIPRI², quoted by AFP, in 2009, 9,1 billion dollars were spent in 54 peace support operations.

In our opinion, in the future, the increase in the costs regarding forces support will become more acute, as a consequence of: the increase in oil costs; the increase in transport costs, on the whole; the development of more and more complex and expensive equipment; the rising standards as far as combatant support is concerned; the adding up of CIMIC activities to all military operations that will take place, the development, in the forecast period, of ISAF (first of all, through increasing the number of combatants).

The elements of logistic support of future operations will definitely have to be adapted to all the armed forces of NATO member states. From this perspective, the Romanian Armed Forces need to modernise their logistic capabilities. This depends both on the will of their leaders and, especially, on the way in which financial resources will find their way towards this field, given the context of the current economic-financial crisis.

Selective Bibliography

- Thomas J. Edwards, Rick Eden, *Velocity Management and the Revolution in Military Logistics*, p. 52, in *Army Logician*, January-February, 1999.
- Gheorghe Minculete, *Opțiuni moderne ale transformării managementului logistic*, în *Gândirea militară românească*, București, no. 4, July-August 2009.
- Bixi Pompiliu Mocanu, *Sprijinul logistic și contribuția sa la asigurarea succesului operațiilor multinaționale*, în *Gândirea militară românească*, București, no. 4, July-August 2009.
- Liviu Scrieciu, *Determinări ale managementului lanțului de aprovizionare-distribuție în logistica multinațională*, în *Gândirea militară românească*, București, no. 4, July-August 2009.
- ***, *Regulamentul logisticii operațiilor întrunite – L1*, București, 2008.

English version by
✍️ *Iulia NĂSTASIE*

² Source: AGERPRES communiqué, 3 June 2010.

SOME OPINIONS ON A POSSIBLE INTEGRATED INFORMATION MANAGEMENT SYSTEM REGARDING COMMUNICATIONS AND INFORMATION TRAINING (II)

Colonel Dr Gheorghe DINCĂ

The general objective of an integrated information management system is to sustain a joint training system that meets the latest Alliance requirements. Such system should bond the unit training with mission requirements, providing, at the same time, the necessary tools for unit training evaluation.

A communication structure that has carried out missions in the theatre of operations has an operational experience that enables it to approach the training process with a different level of understanding the realities specific to the present and the future in the field in which it operates.

Keywords: *operational structure; accessibility; information technology; lessons learned*

In the second part of the article, we continue the presentation of a possible variant of the military training system (figure 1). Thus, if we succinctly analyse the matrix of the training system, we notice the relation between the *mission essential task list (METL)* and the *joint mission essential task list (JMETL)*, as well as the fact that the latter is analysed and revalued within the planning process, at another level of responsibility, with the aim of working out a training plan as appropriate as possible to the mission of the structure. The different training plans that represent the finality of the planning process are taken into account and transformed, during the execution process, into training programmes that facilitate the execution of the training cycle with its components – theoretical and practical ones. The training plans finality as well as the recommendations following the training process are analysed during training evaluation. The finality of this process is usually represented by the enhancement of the training

Colonel Dr Gheorghe Dincă – Commander of the Communication and Information Training Battalion “Frații Buzești” Craiova.

	REQUIREMENTS	PLANNING	EXECUTION	ASSESSMENT
INPUTS	National Military Strategy Strategic capabilities Training directives Alliance commitments National military doctrine Command training* UJTL*	JMETL* TCSRO* Training doctrine Standard operating procedures Annual training plan Lessons learned Command training plan* Training evaluation efficiency* Evaluation training for mission*	Annual training plan* Lessons learned	Annual training plan* Observations on training and evaluation efficiency* Partial results Current operations Lessons learned External determinants Other connections and determinants
PROCESS	Mission performance Tasks identification analysis* Selection of tasks in UJTL* Selection and use of essential criteria JMETL selection* Conditions and standards determination and selection Command and support tasks* JMETL approval by the authority	Command training plan review* JMETL analysis JMETL evaluation review* Training subjects redefinition* Training objectives development Planning training events in relation to resources Publishing some training plans for different structures*	Training cycle execution Development, command and evaluation of the theoretical training events Exercises development, command and evaluation Development/ collection of performances related to meeting requirements Review of performances related to meeting requirements* Establishment of the level of training* Development of post-action analysis*	Training proficiency assessment Review of the lessons learned - from other military actions Preparation of staff and unit evaluation Development of training proficiency analysis* Development of mission training assessment* Draft and development of new lessons learned Identification of the problems related to training
OUTPUTS	JMETL* Tasks, conditions, standards, responsible organisations (TCSRO)*	Annual training plan* Structure of the training ways for different echelons*	Training proficiency evaluations* Tasks performance observations* After action report*	Commander's training guidance Training Proficiency and Mission Training Assessment* Lessons learned validation Training issues definition

Legend: * May be supported by ITIMS
TCSRO = tasks, conditions, standards, responsible organisations
JMETL = joint mission essential task list
UJTL = universal joint task list

Figure 1: Military training system (a possible version)

process efficiency, the establishment of new *lessons learned* and the identification of new problems that should be included in the training plans.

We can highlight, in this context, the fact that some “*outputs*” or “*products*” of the training system are “*inputs*” for the next phases of the process. Following the analysis, we have tried to identify, distinctly marking them, concepts that may be, at the initial stage, included in an *integrated training information management system (ITIMS)*.

Determinants of ITIMS on the individual career management and operational capabilities

Taking into account that such an integrated information system may be structured and may become functional at the level of our armed forces, besides the already presented advantages, we appreciate that it may positively influence not only the individual capabilities management but also the structures one. Tallying all training activities, the “*inputs*” and “*outputs*” in the training management system provides timely and precise information, at any moment, about an individual, group of individuals, a command team or a structure that has been trained or attended a certain course (training sequence).

Thorough data regarding the evolution in career of the professional desired for a certain position may be obtained, the results of the evolution in career, the initial level of training when acceding to a superior level of training, the intellectual and actional efforts made during the training period, the results to tests and complex assessments, the distinguishing qualities someone proves during the training process may be monitored.

Noticing some malfunctions regarding training, the way feedback is provided, the attitude towards resuming some stages or steps in training, as desired results have not been achieved, all these may also be interesting elements for the training process manager as well as for military decision-makers. By extension, such pieces of information that exist in a unitary information system may be useful from the standpoint of the level of training and the capabilities of some monitored communications and information structures.

Monitoring some computer data that exist in the system regarding the training process enables decision-makers and commanders to elicit some elements that determine: the establishment of training needs, the orientation of the staff with a view to drawing up the training plan; the establishment or supplementation of the concept of training execution; the drawing up of the training plan for the superior echelon.

All these elements allow for the information support of the training planning process in order to optimise it to carry out, with minimal costs, the assigned mission. In *figure 2* the stages of the collective training planning for the communications and information structures are presented.

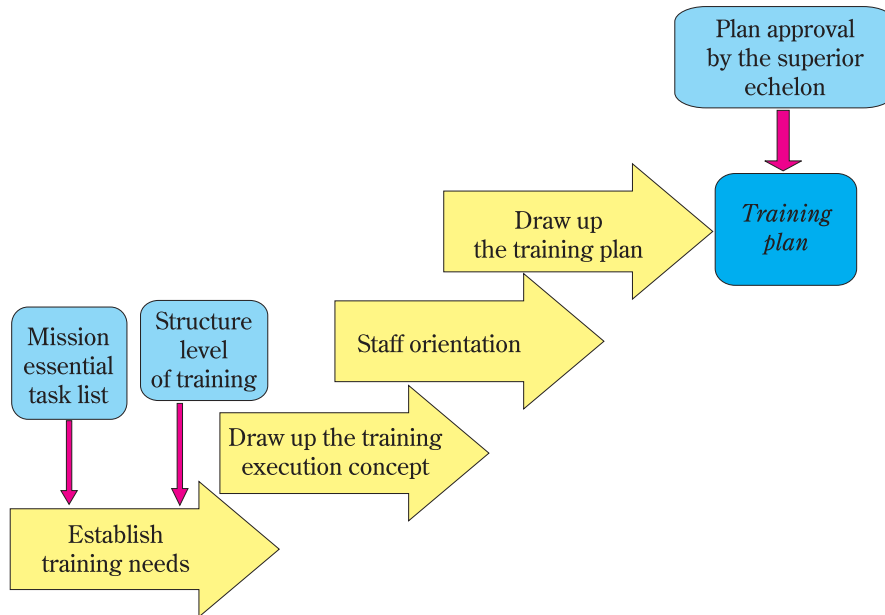


Figure 2: Stages of the planning process for the collective training of a CIS structure (a version)

We appreciate that *ITIMS* may positively determine, through the data it may timely make available to the commander and decision-makers, the following training sequences:

- plans, programmes, training methods and techniques and their effectiveness;
- quality of the subordinate structures commanders and the level of meeting the training process management requirements;
- allocated resources and the effectiveness of their use;
- level of meeting the set objectives;
- level of the structure preparation for the mission;
- training standardisation and evaluation, and problems in the field identification;
- changes regarding the doctrine, procedures, command or force structures and equipment that are necessary for the effectiveness of training activities.

In compliance with the pillars of training – education, training, and training through practice, we consider that *ITIMS* positively determines exercises as a key component of the training process. Through the provided data, the system allows the user to access the information related to the type of exercises – training, evaluation, mission rehearsal, demonstrative ones – the structure takes part in for a certain period, as well as the concordance between exercises, planned objectives, and their specifications. All these pieces of information made available to decision-makers as well as the conclusions drawn following the exploitation of these data allow the planner, commander and other decision-makers to determine the optimal period of training for each echelon in the structure – group, platoon, company; they also allow for the coordination of the activity of the echelons (structures), to eliminate overlaps and deficiencies, as well as the coordination between the collective training and the exercises executed within the communications and information structure.

In order to better understand the relation between collective training and exercises, we have to mention that exercises are executed only by the communications structures that have a high, certified level of training, developed collective skills, those that are trained enough and capable of meeting the set performance standards.

Exercises can be planned only after the collective training stage is completed and they presuppose the performance of some activities that are similar to the ones meant to carry out real missions. These are some elements that support the statement according to which exercises are more related to operations than to training and, for a better presentation of their relation with collective training, we illustrate, in *figure 3*, the time allocation for the training of each echelon belonging to a communications and information structure.

The data provided by *ITIMS* regarding the coordinated execution of training may lead to multi-echelon training from the platoon up to superior levels. The proposed system also offers important data related to training through practice, the positions a professional has filled after the period of institutionalised training, the experience acquired through periodically taking part in actions in the theatres of operations. We appreciate that the data provided by the proposed information system may be interchangeable with the ones of the military education system and they may optimise the future career of each and every military man through projecting, organising and developing his training. The effects of training through practice, monitored by *ITIMS*, may be detected not only at the level of the expert in communications and information but also at the level of military structures. A communication structure that has carried out missions in the theatre of operations has an operational experience that allows it to approach the training

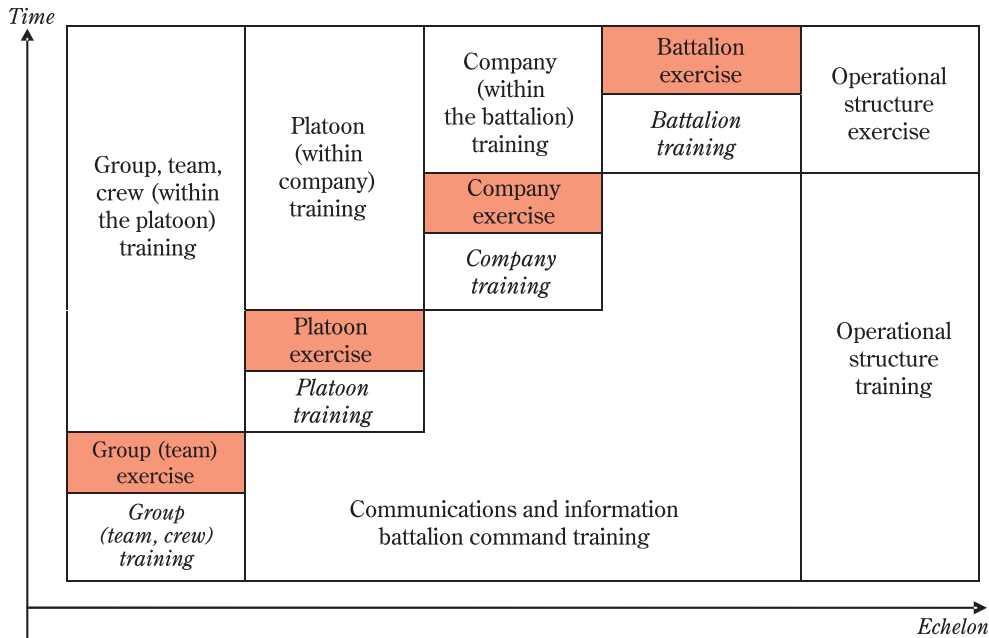


Figure 3: Synchronisation between collective training and exercises

process with another level of understanding the realities specific to the present and the future in the field in which it performs its activity.

In *figure 4* we present the *ITIMS* process, with its probable stages: *planning, analysis, study, development, implementation, maintenance* and *development*.

Mention should be made that the proposed system is a logical one that develops successively, from simple to complex, and it is tested in practice at different time intervals, usually following upgrading. The system management is performed by soft experts in close cooperation with experts in operations and training to manage the processes of the system in compliance with the requirements of training processes, training categories, participants in training, as well as with the periodicity of training sequences in conformity with the training plan.

Key responsibilities fall under the staffs regarding the development of some requirements and standardised documents to determine performance indicators, basic characteristics of the training process, time norm, performance levels and other details, as well as under the experts in information technology to establish the hardware structure, to design software meant to introduce and extract data from the system and to establish the methods, techniques and procedures employed to process and store information.

Among the facilities offered – elimination of subjectivism in assessment, comparative verification of some training plans, comparative analysis of some similar

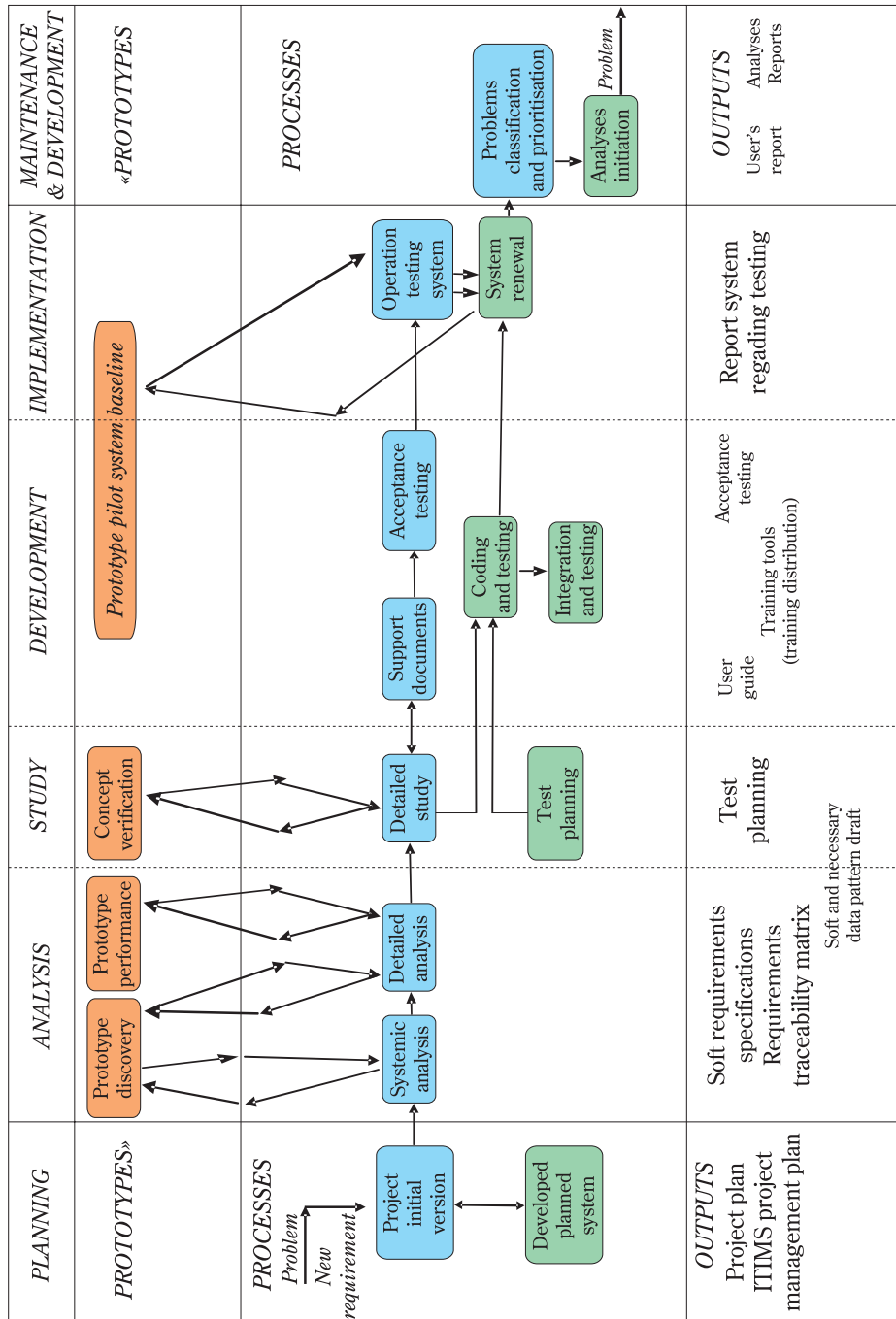


Figure 4: ITIMS process management

structures or of some different structures that have attended similar training programmes, identification and verification of more training versions having the opportunity to select the optimal version for a given situation, rapid exchange of a consistent volume of data and information related to training, conclusions regarding the evolution of some training structures and systems –, we can advance the opinion that such a system may tend to be an expert system.

The above-presented facts allow us to appreciate that *ITIMS* may determine the implementation of new educational software, the initial training of the new members of the “*training community*” with a view to providing abilities to use the entire system, may facilitate the refreshment of training for those who have experience in training, as well as the training and certification of trainers for the current and future training capabilities.

Training through *ITIMS* will be influenced by not only the use of classical training teams but also by the facilities offered by the distributed training technology, allowing for the use of information and communications technology to transfer knowledge in standard format¹. The benefits of the system are the same with the ones of the advanced distributed learning: accessibility; interoperability; further use; durability; effectiveness.

In *figure 5*, *ITIMS* potential beneficiaries and the training categories that may be accessed by each beneficiary are presented.

ROLE	TRAINING TYPES					
	Establish a vision regarding the system	Implement new training versions	Initial training (new users)	Training refreshment (experienced users)	Trainers training	Training and training information management
<i>Common users</i>			X	X		
<i>Analysts</i>			X	X		
<i>Group of users</i>	X		X	X		X
<i>Trainers</i>	X	X			X	X
<i>ITIMS specialists</i>	X	X				
<i>Leaders</i>	X		X	X		X

Figure 5: Training audience and training categories

¹ Ion Roceanu, *Elemente de bază ale unui sistem e-Learning bazat pe principiile ADL*. Scientific communications session – Section e-Learning and educational software, Editura U.N.Ap., București, 2005.

Starting from the current validity of the words of Lieutenant General Ervin J. Rokke, USAF, related to the fact that *“lessons are only truly learned when we incorporate them into our planning, doctrine, tactics and training”*, we can appreciate, in some ideas, the extraordinary determinants such a system may produce in the particular field of training experts in communications and information as well as of the branch specialised structures:

- the achievement of a *lessons learned* management package in the field of communications and information, at the branch level, would be the first step in ensuring a considerable volume of data necessary for the structures and experts that have training responsibilities;
- combination of all the data related to the exercises like *Combined Endeavor* (interoperability exercises in the domains – command, control, communications and computers of the technical systems in NATO and PfP member countries) – in order to provide a forum to exchange information regarding equipment, communications and information systems and their capacity to interoperate with the ones belonging to other nations, as well as to create an interoperability guide to be used by operational planners and the technical personnel in the combat area² – may represent a preliminary stage in the achievement of a training-related information joint management system;
- automation of the training process four phases (requirements establishment, planning, execution and evaluation) with their integration in a single software package will facilitate the achievement of an *ITIMS* that will significantly influence the way training in the field of communications and information is planned, organised and developed³;
- the Romanian military education system transformation is a reality, under the circumstances of the integrated transformation of the Alliance, the Romanian Armed Forces, having consequences on some education systems that are specific, interconnected, possibly joint ones in a network that facilitates the educational content compatibility and the knowledge distribution following the principle: *To whom ?*, *Where ?* and *When is it necessary ?* – *“A supplementary argument for the reciprocal determinations of the transformations occurred in military affairs and education in the military*

² Cristea Dumitru, *Sisteme – C4I*, Editura Militară, București, 2005.

³ Gheorghe Dincă, *Politici de formare și perfecționare profesională a specialiștilor și structurilor de comunicații în armatele altor state membre și nemembre NATO*, Editura U.N.Ap., București, 2005.

domain is represented, maybe not accidentally, by the fact that the two concepts considered revolutionary (Network-Centric Warfare – NCW and Advanced Distributed Learning – ADL) were both launched in the same year, 1997⁴.

In conclusion, stating that the idea of achieving an integrated training information management system may generate important and desirable transformations in the communications and information training system, we mention that the new and modern training system in the branch has to be characterised by simplicity that allows for immediate assessment. Moreover, it has to be efficient up to the maximum, a self-regulatory system, oriented towards novelty and performance in order to meet the set fundamental goal – *victory in the military action*.

English version by
✍️ *Diana Cristiana LUPU*



⁴ Ion Roceanu, *op. cit.*

ECONOMIC AND SOCIAL THREATS TO INTERNATIONAL SECURITY

Dr Irina CUCU

In the beginning, the author presents the new types of conflicts, the economic ones, which do not trigger the direct loss of lives, yet, make more and more “collateral victims”. Then, it is shown that the experience of the most recent conflicts worldwide shows that, after the failure of diplomacy and coercive diplomacy, states frequently resort to other instruments of power: information, economic and military ones. Moreover, it is mentioned that conflicts not only destroy infrastructure but also encourage crime, hinder investments and make normal economic activities impossible. Unfortunately, as long as there are wars, the military purposes will be more important than social or ecological issues. The social or surrounding environment will never be entirely protected from the military risks. Yet, considering the serious situations that may occur with time (to mention only global warming), one can consider at least the reduction of the devastating effects of war.

Keywords: *economic conflicts; intelligent weapons; social security; consumerist spirit; economic security*

The place of military conflicts has been currently taken by the economic ones. It is a well-known fact that, from ancient times, the purpose of all wars has been economic; yet, today, the fight is not carried only between state players, but especially between non-state ones.

These new types of conflicts do not trigger the direct loss of the lives of a considerable number of combatants, yet, “*collateral victims*” and material losses are more and more numerous and bigger.

The experience of the most recent conflicts worldwide shows that, after the failure of diplomacy and coercive diplomacy, states frequently resort to the other instruments of power, the information, economic and military ones¹.

Current conflicts, whatever their nature may be, even if of small proportions, have not ceased; confrontations, irrespective of the degree of violence and the number of states involved, take place all over the planet.

Security is a prerequisite for development. Conflicts not only destroy infrastructure, social infrastructure included, but also encourage crime,

Dr Irina Cucu – Centre for Defence and Security Strategic Studies/“Carol I” National Defence University.

¹ Teodor Frunzeti, *Geostrategie*, Editura CTEA, București, 2009, pp. 51-53.

hinder investments and make normal economic activities impossible. A series of countries and regions are caught up in a cycle of conflicts, insecurity and poverty. The competition for natural resources – especially for water –, which will be aggravated in the following decades as a consequence of global warming, may cause turbulence and supplementary migrations in many regions².

One cannot yet establish what the dominant type of conflict in the current millennium will be, yet, it is certain that conventional wars are not so spread anymore; their place is more and more taken by “*modern wars*”. The place of “*conventional*” weapons from the 20th century is taken now, at the beginning of a century and of a millennium, by “*intelligent weapons*”. In this respect, an important weapon employed in economic conflicts, preponderantly used in contemporary market economy, is the psychological one, aimed at national psychology elements: changing mentalities, aspirations, ideals, ideas, theories, behaviours, morals. For this purpose, manipulation methods are used that are very difficult to identify, based on the exploitation of basic instincts (food, defence, reproduction necessity) and primitive inclinations of the human being. Conflicts are determined by the competition for economic goods and the differential distribution of authority in society.

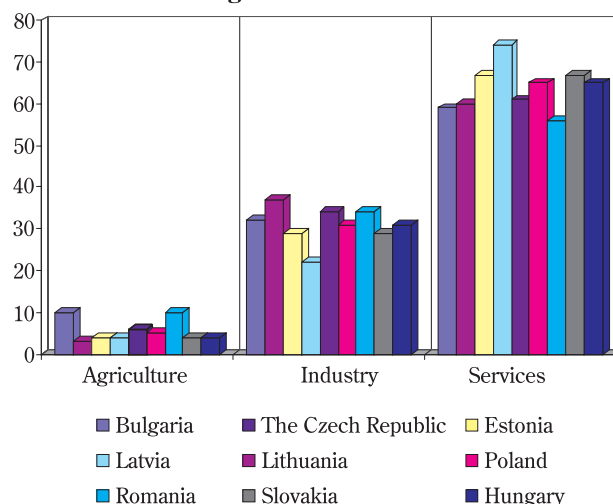
Those interested – institutions, organisations or persons – in manipulating people take different courses of action with a view to reaching the set objectives in the short, middle and long term. Thus, one of the courses of action is the ***inoculation and development of the consumerist spirit*** to as many people as possible, to the prejudice of the spirit of economy and moderation. To this end, the manipulating source resorts to: manipulating commercials; awakening predatory instincts; exploiting vanity, shallowness, naivety and other negative personality traits. It is known that, in order to lead a normal life, every human being has a complex of needs. The economic aggressor aims to develop artificial needs and requirements into the target-human being and the target-nation, to take their last penny from their pocket or from their banks, to make them go broke, dependent on loans that are given by the manipulator itself. Therefore, if the target-individual and/or the target-nation do not resist the carefully shaped temptations, they will become economic slaves. This phenomenon can also be noticed in Romania. Currently, we consume more and more products, luxury ones included, from import, and banks have outdone themselves in offering many apparently advantageous loans. This has led to an explosive increase in prices, especially in the real estate sector, in which things got out of proportions. Moreover, the increase in the consumerist trends

² <http://www.consilium.europa.eu/uedocs/cmsUpload/031208ESSIIRO.pdf>

has made many people run into significant debts, some of them even lifelong, and that is why the dependence of the individual or even the entire nation on the banking system has increased significantly.

Another course of action is **diverting the attraction and interest of citizens from the economic, material sector, which produces goods and values**, to unproductive or harmful directions. In our country, one can currently notice an inflation of overcrowded supermarkets, which sell important products every day, provide jobs but, practically, do not produce commodities in order to somehow compensate for the imports. That is why one can say that their contribution to the enduring development of the country is not significant.

The Contribution of Main Activities to Achieving Gross Value Added in 2009



In 2009, the main contribution to the Gross Domestic Product of the Eastern European countries was made in the services sector (mostly from trade). This is further proof of the victory of multinational companies, whose purpose has been to monopolise the markets worldwide and to eliminate small national companies.

At the same time, a priority course of action of manipulators is the creation and inoculation in the collective consciousness (and unconsciousness) of the target-nation **of certain human and technical values that are false or are not proper to the national values validated by the social practice**, with the purpose of replacing traditional values.

Moreover, an important course of action on the part of manipulators consists in **destroying the image of certain leaders or politicians** who fight for the economic

development of their nation, on the one hand, and their ***intoxication with false information*** regarding a domain they must lead, especially the economic one, on the other hand.

The factors that provide economic security both at the micro and at the macro social levels are: housing safety; job safety; minimum income safety; economic competitiveness; sovereignty and food security (on the one hand, the need for providing the access of every individual to food, eventually the self-sufficiency of agricultural production and, on the other hand, the quality of food); universal social protection (first, for the most disadvantaged ones), which requires state aid, safety of pensions; access to education and medical services³.

In the opinion of experts in security studies (Barry Buzan, Ole Weaver, Jaap de Wilde), the modern concept of security includes five cumulating factors. The security of a state entity is provided if each of the following five security components is taken into account: the political, military, economic, social and ecological ones.

Economic security refers to access to resources, funding and markets that are necessary in support of the acceptable levels of the development and power of the state. When speaking of social security, we think of maintaining, within the framework of certain conditions that are acceptable to make possible the evolution process, the collective national identity, the traditional models of the language, culture, religion and other customs proper to a people. Looking at how things evolve, some of the biggest problems for European security will be posed by the social component, because of the situations in Bosnia Herzegovina, Transnistria, Macedonia, Kosovo, Belarus, Montenegro. The security of the environment is related to maintaining the planetary biosphere at the local level, as an essential support of the system on which all the other human activities depend⁴.

Other risks with major impact on economic security are social risks: increasing unemployment, *“under the table”* jobs and legislative risks: instability and ambiguity of certain legal regulations, regulation of crimes and contraventions without a clear delineation between them.

The consequences of business crime, visible at the social, political and juridical level, represent real social bombs (e. g. FNI – the National Investment Fund), as they are embodied in a state of modern social-economic dependency

³ *Ibid*, p. 35.

⁴ Barry Buzan, Ole Weaver, Jaap de Wilde, *Security. A New Framework for Analysis*, Lynne Reiner Publishers Inc., London, 1998, pp. 7-8.

with demoralising effects for the population and of deterioration of the trust in state institutions.

At the same time with the integration in the European common market, with the development of the freedom of movement of commodities, persons, services, favourable conditions are created for frauds at the European level, characterised by a sophisticated, occult *modus operandi*⁵.

Conflicts affect more and more the civil population. Even if the number of armed conflicts has decreased, current wars are much more brutal, long-lasting, difficult to settle and, most importantly, they involve more and more civilians. However, the changes occurred in the nature of security threats and, implicitly, in the concept of security have had an effect on the relation between the military and the civilian sector in crisis and international conflicts management, the latter one gaining a more and more important role⁶.

Children are the most innocent victims of conflicts. It is estimated that, only during the last decade, armed conflicts cost the life of over two million children and mutilated other six million. Conflicts made children orphans, deprived them of care, basic social services, medical assistance and education. There are approximately twenty million displaced or refugee children, while others are taken hostage or made victims of trafficking. The systems regarding birth registration and justice for minors do not work. It is estimated that, at any moment, there are at least 300 000 child soldiers who participate in conflicts⁷.

To have control of resources, markets, high technologies, even of “*brains*”, both states and large companies use any means, often irrespective of the consequences of this fight. In this context, the possession, availability and effective use of natural resources, especially energy ones, is a source of tensions, crises or even conflicts. For these reasons, natural resources have represented the subject of extensive international debates about both their existence and distribution. However, the implications produced by the “*rush for profit*” have disastrous environment consequences. All these have repercussions on social and international security, starting from the security of the individual, of the nation to the global one. Disasters that occur in certain areas cause crises/conflicts, which, because of the lack of vital resources, can transform into regional and beyond conflicts.

⁵ Gheorghe Văduva ș.a., *Securitatea sistemelor și acțiunilor militare și civil-militare în gestionarea crizelor și conflictelor armate*, Proiectul CEEX-M1-4044-Gestionare CF-16/2006, NDU Library.

⁶ ***, *Gestionarea crizelor și a conflictelor internaționale*, <http://www.scribd.com/doc/25048501/Gestionarea-Crizelor-Si-Conflictelor-Inter-Nation-Ale>

⁷ ***, *EU Guidelines on Children and Armed Conflict*, <http://www.consilium.europa.eu/uedocs/cmsUpload/10019.ro08.pdf>

If nature could provide unlimited material, energy and food resources and turn them into economic goods, then the relation human being – nature, as well as the inter-human relations in any country would have a different content. Reality shows that, in the context of the limitation of these resources, a real strategy is needed to meet the need for such goods, the human and social factor fundamentally adding to the natural one.

Crime activities can turn into the most dangerous activities generating illicit incomes, namely: drug trafficking, human trafficking, major frauds, business crimes, which are genuine *sources of social and economic insecurity*⁸.

The main indicators through which the level of *social security* is measured, in different domains, are:

- *the social indicators of housing*: housing stock (number of residential units reported to 1 000 inhabitants, the number of rooms reported to 1 000 inhabitants, the average habitable surface reported to a person), the development of the real estate sector (the involvement of the public sector in housing projects, the infrastructure expenditure that falls under a person in a year in the urban environment), the housing conditions (the rate of the urban population, the rate of the population living in pollution-affected areas, the mortality caused by environment pollution, the rate of housing with potable water);
- *the social indicators of poverty*: the poverty threshold, subsistence minimum, poverty rate, poverty gap, *Sen index* (the percent of the total income of the population that should be transferred to the poor, so that their income could be brought at the level of the poverty threshold), *Fishlow index* (it expresses the poverty gap, as a percent from the incomes of the non-poor, in the idea of eliminating poverty through direct transfers of income from them), *Gini coefficient* (it measures the inequality of incomes) etc.;
- *the indicators of the health status*: the morbidity rate, morbidity by classes, access to health services, provision of the population with doctors, pharmacists, indicator of human resource provision etc.;
- *the indicators of human freedom and development*: the indicator of human freedom, indicator of human development;
- *the indicators for the characterisation of the education system*: the enrolment rate, internal efficiency of the education system, quality of education services and use of resources etc.⁹.

⁸ Danusia Aurelia Boicean, *Criminalitatea și economia subterană, factori de risc pentru creșterea criminalității economice*, in *Studia Securitatis*, no. 1/2007.

⁹ E. Bădălan, E. Mavriș, *Dinamică și tendințe în transformarea sistemelor de securitate*, in "Anuar 2007", Academia Forțelor Terestre, vol. 1, 2007, p. 86.

The main domains that can generate social crisis situations are: social exclusion; low standard of living, perpetuation of unsolved ethnic conflicts; absence of civil society organisations; tensions related to language, religion, ethnic group; failure of decision-making mechanisms/increase in authority legitimacy¹⁰.

The social indicators for assessing the sources, states and dynamics of crisis situations and conflicts: labour employment (unemployment level and dynamics); social assistance; education level; training, cultural level of the population; civilisation level; social attitude; stability; normality or resurgence of social unrest; trade union activity; social condition of the family. Demographic indicators can also be included: birth rate dynamics; mortality rate dynamics; age ratio dynamics; migration phenomenon; population stability or instability; abrupt changes in the ratio between urban and rural population; populations exodus¹¹.

Security is a social phenomenon that involves two types of social determinants: general and specific to conflict/war ones.

General determinants are represented by social tensions that are increasing and generate crises/conflicts. At the same time, in certain conditions and social environments, interests occur, placing one part of the human community against the other, or the vindictive, warrior spirit appears or escalates within certain ethnic groups or national minorities.

Specific determinants are generated by the enlargement of the vital space of an entity, the occurrence and sustainment of the aggressive or revengeful spirit, the manifestation of certain economic interests with determinants in the social environment. All these determinants only partially explain the state of security/insecurity. The conflict/war represents, in fact, a social liberation/relief of energies and tensions, and its effect appears as a new social balance or as a social restructuring. Insecurity can also occur as a consequence of social anomie, as a product of certain group interests, as in the case of terrorist war. At the same time, the social environment also generates the anti-war-like, pacification spirit, in order to preserve the security environment.

Mention should be made that the social environment is not immutable, but it is changing, depending on the economic, political, information determinants. The acceleration of the economic growth is first aimed at providing the prosperity of citizens and supporting the internal democratic process. Increasing people's confidence in state institutions is possible only in the circumstances of the constant

¹⁰ I. Voievozeanu, C. Romanoschi, *Managementul crizelor din domeniul politico-militar*, in "STRATEGII XXI", 2007.

¹¹ *Securitatea sistemelor și acțiunilor militare și civil-militare în gestionarea crizelor și conflictelor armate*, CEEEX-M1-4044 Research Project, 2009.

promotion of the principles of the rule of law and of the fundamental rights of the citizen.

Unfortunately, as long as there are wars, the military purposes will be more important than social or ecological issues. The social or surrounding environment will never be entirely protected from the military risks. Yet, considering the serious situations that may occur with time, and which have already begun to make their presence felt (to mention only global warming), one can consider at least the reduction of the devastating effects of war.

Considering the presented facts, not only the armed conflicts have an effect on the social and surrounding environment, but also the economic ones. In the rush for gaining profit and getting rich fast, as long as competition is fierce, the big companies will forget about environmental protection, spilling various substances in the surrounding environment and affecting it as far as space and time are concerned.

English version by
Iulia NĂSTASIE





CYBER WAR AND CYBER POWER. ISSUES FOR NATO DOCTRINE

Dr Jeffrey HUNKER

In this research paper, the author focuses on some terms that are extremely used in the current international security debate and were intensely used in the discussions regarding NATO's New Strategic Concept: cyber space, cyber threats, cyber attacks, cyber terrorism and cyber weapons.

First, the author defines the types of cyber attacks, as well as the concepts of cyber warfare and cyber power. Then, he writes about the number of challenges presented by the use of cyber power.

In the end, he draws attention to the implications of cyber war for NATO, pointing out that the Alliance needs to develop a clear doctrine of cyber power, addressing issues of offensive use, defence, response and deterrence.

Keywords: *cyber war; cyber power; NATO; security & defence; US Cyber Command; offensive operations*

“Cyber war” is now the subject of considerable attention in the US, both in the popular media and in policy realms (together with its companions, *cyber threats, cyber attacks, cyber terrorism, and cyber weapons*). For those in NATO it is important to understand what cyber war and related terms mean, why they are the subject of US focus, and what the implications for NATO are. That is the purpose of this paper.

The combination of extensive dependence on cyber systems and the pervasive security vulnerabilities in these systems is the foundation for the growing concern about cyber war and other cyber threats. Unfortunately, one challenge of discussing cyber war is that there are few, if any, commonly shared definitions or clear-cut distinctions between key concepts. *When is a cyber attack an act of war or a crime? Indeed, when is an unauthorised penetration of a cyber system*

The article was published in the *Research Paper* no. 62, November 2010, of the Research Division at the NATO Defence College, Rome, www.ndc.nato.int, e-mail: research@ndc.nato.int. The intellectual property rights of the paper remain vested solely in the NATO Defence College (© NDC 2010 all rights reserved).

Dr Jeffrey Hunker – Principal of Jeffrey Hunker Associates LLC, Pittsburgh Pennsylvania, USA. hunker@jeffreyhunker.com. He is author of *Creeping Failure: How We Broke the Internet and What We Can Do to Fix It*, McClelland and Stewart, 2010. The views expressed in this paper are the responsibility of the author and should not be attributed to the NATO Defence College or the North Atlantic Treaty Organisation.

a cyber attack ? What are cyber weapons ? How would the attacked know where a cyber attack originated from, or even that they are being attacked, and what degree of confidence is required to respond ? What responses are legal, or appropriate ? And, from the adversary's perspective, how does the attacker know if a cyber attack will be successful ?

This paper first explains the basis for concern about threats to cyber systems, and distinguishes between the different types of cyber threats and attacks. I define cyber attack and other key concepts, fully aware that there are many alternative definitions, and then review the history of events that relate to cyber war. In doing so, I will introduce the concept of cyber power.

A key conclusion of this paper is that, for NATO, cyber war as the focus of concern is a misnomer; the real or potential use of cyber power by nations or terrorist groups should be the principle focus. Cyber war is just one outcome of the exercise of cyber power between nations. The central part of the paper will outline some of the special characteristics that distinguish cyber power from the other elements of national power, and point to some of the challenges that these special characteristics present in developing a doctrine of cyber power.

I will then briefly review NATO and US policy relating to cyber power, and point to the need by NATO and NATO members to develop a cyber power doctrine, supported by coherent foreign policies.

Dependence and Vulnerabilities in Cyber Space

Cyber space is the notional environment in which digitised information is stored or communicated over information systems and networks. Largely because of the Internet, in a very short time – less than twenty years – much of what goes on in advanced countries depends on cyber space. Critical infrastructures like pipelines and many industrial processes now run on *Supervisory Control and Data Acquisition (SCADA) systems*, many of which are connected through the Internet¹. Whether a phone call is on *Skype*, cellular or normal phones, much of long distance telecommunications is routed either on the Internet or through the same fiber optic cables carrying Internet traffic.

Cyber space is rife with vulnerabilities – ways in which malicious actors can cause cyber systems to behave in manners in which they were not intended to behave. Vulnerabilities may be due to design error, or inherent in the design of the systems, and may overlap with “bugs”, which are defects that may also cause accidents. Vulnerabilities exist at the system level, e.g. in desktop software.

¹ The Stuxnet Worm first observed in September 2010 is reported in the press to have been intended to target and disable the SCADA systems of Iran's first nuclear power plant. This is the first (?) high profile example of a cyber attack specifically against SCADA systems.

Vulnerabilities also occur at the network level. The Internet, for instance, depends on the *Domain Name Service (DNS)* to look up network addresses; the DNS ultimately runs on 13 computers which, if malfunctioning, would disrupt, albeit slowly, the workings of the Internet. *Distributed Denial of Service (DDOS)* attacks rely on massive floods of incoming data packets² to prevent users from accessing systems, without actually harming the systems affected directly. Despite much attention to reducing vulnerabilities, cyber space will remain exposed to malicious attacks.

Exploiting Vulnerabilities: Defining Types of Cyber Attacks

There are many ways of exploiting vulnerabilities – from the attacker on another continent remotely inserting malicious software into a system to a co-worker stealing a password. However done, the act of exploiting or attempting to exploit a vulnerability without authorisation is a *cyber attack* (this is my definition; there is no consistent terminology here). Since there are so many ways of exploiting vulnerabilities – i.e. launching a cyber attack – the term “*cyber weapon*” is meaningless in general usage.

The goal of a cyber attack can be to either:

- copy and then remove data without disrupting the systems or data – a *passive cyber attack*³ – or
- disrupt cyber space systems by corrupting or changing data, affecting system or network service, or denying or preventing use of systems or networks – a *disruptive cyber attack*⁴.

A passive cyber attack could either be a cyber crime, e.g. theft of passwords or credit card data, or cyber espionage or intelligence collection if done by a state. Cyber crimes could also be committed by terrorists, as for example committing cyber theft in order to raise funds for operations.

A disruptive cyber attack could be a cyber crime committed for greed, vandalism, revenge or extortion, or could be an act by terrorists, non-state actors or a state.

² The Internet transmits messages/information by breaking the message into many discrete data packets, each of which may be sent across the Internet using different paths to arrive at the final destination, where the Internet Protocol reassembles the packets to reform the original message.

³ The US DOD uses the terminology “*computer network exploitation*” and “*computer network attack*” for passive and disruptive cyber attack; attacks need not involve networks (although they usually do), and “*exploitation*” is less clear than the intended effect, which is to be passive, leaving the system undisturbed.

⁴ A fuller definition of nation-state disruptive cyber attack: the unauthorised penetration, use, or denial of use by a nation-state (or its proxies) of another nation’s cyber systems (whether government or private) for the purpose of causing the disruption of or damage to these systems or their use, or the systems (including physical infrastructures) which these systems control. This definition is mine, but is based on elements of other definitions.

Disruptive cyber attacks could have potentially serious physical consequences with social and economic implications; for instance, electrical power systems and rail lines are managed through cyber space. US policy names eighteen economic sectors as critical infrastructures whose functioning is essential for security, economic and social welfare; most of these critical infrastructures, including information technology, telecommunications, electric power and oil and gas depend in large part on cyber systems for their operation. A recent US government inquiry into the cyber security of one large electric utility found significant vulnerabilities that left it open to cyber attack. US policy makers are concerned about the vulnerability of military systems too: in 1997, the Eligible Receiver exercise aimed at testing the Pentagon's cyber security; within two days attack teams had penetrated the classified command network and were in a position to issue bogus orders.

With valuable information and key services dependent on cyber systems, not surprisingly cyber crime in all forms has grown rapidly and is now the province of sophisticated criminal organisations operating globally. Total cyber-related business losses in 2009 are estimated to be US\$ 42 billion for the United States, and US\$ 140 billion globally⁵.

Cyber espionage, too, is a major threat. US counter-intelligence officials estimate that 140 different foreign intelligence agencies regularly attempt to hack into US commercial and government computers. Note that cyber espionage sometimes occupies a grey area between passive and disruptive forms of cyber attack. While traditional espionage per se does not appear to violate international law, many of the technical means of conducting cyber espionage (e.g. by implanting malicious software into the target systems) are close to or almost identical with the technical means of mounting a disruptive attack on the same system. Also, the amount of data that can be obtained and the speed of cyber espionage can be of a different order of magnitude from that of more traditional espionage operations. In April 2009, someone illicitly downloaded terabytes of information from US national security computers related to the development of the F-35. With a high degree of certainty, these officials believe that the intrusion can be traced back to an Internet address in China and that the signature of the attack implicates Chinese government involvement⁶.

⁵ Estimated losses due to cyber crime are highly unreliable; many businesses prefer not to report cyber crime. Cyber crime has exploded since 2000 and has become a form of organised crime. D.C. Blair, *Annual Threat Assessment of the Intelligence Community for the House Permanent Select Committee on Intelligence*, Washington, Director of National Intelligence, 2009, <http://intelligence.senate.gov/090212/blair.pdf> (accessed 27 September 2010).

⁶ Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do about It*, New York, HarperCollins, 2010, p. 233.

In parallel with cyber espionage capabilities, reportedly many nations have been developing disruptive cyber attack capabilities. China is a sophisticated cyber state, having recently surpassed the US in the number of Internet users. China talks of “winning informationised wars by the mid-21st century” and is, according to US analysis, developing “an advanced information warfare capability, the stated goal of which is to establish control on an adversary’s information flow and maintain dominance in cyberspace”. In April 2009, the Wall Street Journal reported that China had planted logic bombs⁷ in the US electric grid. Many other countries are building up disruptive cyber attack capability, among them Russia, Israel, and North Korea⁸.

Incidents of Cyber War ?

Almost certainly, we have already seen disruptive cyber attacks by one nation against another nation, though I am unaware of any cases of terrorist groups launching disruptive cyber attacks. Some of these events have been described as *cyber war*. The following are select instances:

In May 1999, following the accidental bombing of the Chinese embassy in Belgrade, Chinese hackers targeted US government web sites; the White House shut down www.whitehouse.gov for three days because of security concerns stemming from the non-stop DDOS attacks.

In 2007, during a period of tension with Russia, Estonian government, commercial and private organisations, notably banks, were the subject of three weeks of DDOS attacks. Other DDOS attacks occurred against Georgia in 2009, prior to kinetic military action with Russia, and against Kyrgyzstan in 2009. In all cases, the likely governments – China and Russia respectively – denied any involvement; the cyber attacks against Georgia were orchestrated from a control computer in Brooklyn, New York City.

Reportedly, also in 2007, Israeli jets bombed a complex in eastern Syria. Under construction with a North Korean labour force, the complex was to have been a North Korean-designed nuclear weapons plant. Israeli jets were able to penetrate Syrian air space without detection, having somehow evaded or subverted sophisticated air defence networks (provided by the Russians) through a cyber attack⁹.

⁷ A logic bomb is a piece of software intentionally and maliciously inserted into a software system (e.g. a computer) that will damage or destroy the system’s functionality when a specific condition occurs (e.g. a certain date is reached) or by command.

⁸ A thorough recent discussion of Chinese capabilities is Steve DeWeese et al, “*Capability of the People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*”, Report prepared by Northrop Grumman Corp. for the US-China Economic and Security Review Commission, Washington, 17 February 2010, www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FinalApprovedReporM60ct2009.pdf (accessed 27 September 2010). See also “*War in the Fifth Dimension: Briefing on Cyber war*”, *The Economist*, 3 July 2010, pp. 25-28.

⁹ Clarke, *op. cit.* (who provides no citations to support his material).

To summarise, the combination of dependence on and vulnerabilities in cyber space, together with a growing record of cyber attacks exploiting these vulnerabilities, supports the perception that cyber space is a realm where national interests – military, diplomatic, economic and social – are now at risk.

The Concept of Cyber Power

The focus of NATO concern should not just be cyber war per se but rather the direct or threatened exercise of *cyber power* through computer network attacks. While attractive in the media, cyber war is a special form of disruptive cyber attack¹⁰:

- *Cyber warfare* is a serious form of disruptive cyber attack by a nation on another nation's cyber space, crossing the line into being considered a use of force. Issues of the Law of War come into play.

Note that an act of cyber war is only one outcome of a nation launching a disruptive cyber attack. Cyber power as a concept covers more completely aspects of concern to NATO:

- *Cyber power* is the use, threatened use, or effect by the knowledge of its potential use, of disruptive cyber attack capabilities by a state¹¹.

It is worth pointing out that most discussions of "*cyber war*" reference instances of disruptive cyber attack where the parties neither enter into nor are already in a state of armed hostilities; the Georgian attack is an exception. In other words, most discussions are not about war but about the use of power.

Nations may project cyber power in many ways – in concert with other kinetic military operations, masked and with no clear link to the attacker, as part of a complex military-diplomatic escalation, or in indirect manners to exert influence or advance national goals. Note that passive cyber attacks – meaning mostly espionage – are not elements of cyber power, just as non-cyber espionage is not an element of national power as usually defined. Massive cyber espionage

¹⁰ Military doctrine categorises the four elements of national power under the acronym "*DIME*" – *Diplomatic, Information, Military and Economic*. "*Information*" as an element of national power describes a grab bag; for the US Defense Department "*information operations*" include electronic warfare, psychological operations, military deception, operations security and computer network operations. Computer Network Operations – the topic of this paper – is further divided into computer network attack, computer network defence and related computer network exploitation enabling operations to be conducted. I would argue that the special characteristics of cyber power and cyber space (to be discussed shortly) support cyber power as a fifth element of national power. Cyber space is neither a physical realm (where military operations have historically taken place) nor a perceptual sphere (e.g. that of "*psych ops*"). The closest historical analogy to disruptive cyber attack might be, for example, the scrambling or distortion of adversary radio communications. The potential scope and impact of cyber attacks is so much greater than what might be seen in historical analogies to again argue that cyber should be considered a fifth element of national power.

¹¹ See also Franklin D. Kramer et al, *Cyberpower and National Security*, Washington, Center for Technology and National Security Policy, National Defense University Press, Potomac Books, 2009, p. 48.

programs, or the technical means of conducting cyber espionage that could be perceived by the target as tools of disruptive cyber attack, are “grey areas” for how cyber espionage might be regarded.

Cyber power has some unique characteristics which shape its effective use:

Cyber space is a wide and dynamic environment. The pace at which change occurs far exceeds that of almost all physical systems. Change is not just in technological innovations; transformations are ongoing in network and system configurations, uses, and social/organisational interactions. Detailed maps of cyber space, if any existed, would almost immediately become obsolete.

Cyber weapons, once used, often lose their effectiveness: many cyber attacks depend on exploiting vulnerabilities unknown or unpatched – i.e. not fixed – by the target. Once a particular vulnerability has been exploited, especially in a noteworthy cyber attack, most likely that vulnerability will be patched, and the particular cyber weapon will lose its effectiveness. This is not universally true; for example, DDOS attacks do not depend on vulnerabilities in the target system, and in effect there are no good defences against these types of attacks.

Offensive operations dominate in cyber space: the challenge to defence is to patch all vulnerabilities; the attacker’s opportunity lies in finding only a single key vulnerability in complex systems. There is no indication that this inherent attacker advantage will change in the foreseeable future.

Cyber operations can occur at the speed of light: physical constraints related to the use of kinetic weapons do not apply to cyber attacks.

Cyber attacks have global dimensions: almost by definition, given the topology of cyber networks, cyber attacks will transit nations other than just the attacker and target. This can create challenges (discussed later) in identifying the true source of an attack – a cyber trail may grow cold at an intermediate location with no resolution as to the true attack source. Or, cyber attacks can be mounted from cyber systems located in countries other than the attacker – with or without the knowledge of the other state or system owner). The physical and technical resources required for an attack are not necessarily large enough to generate special notice, even if operating in another country.

Disruptive Cyber Attack in Combination with other Attack Modes

I would further argue that *disruptive cyber attacks* conducted without any kinetic accompaniment do not make much sense in large-scale warfare. Disruptive cyber attacks can destroy important data and disrupt communications, and perhaps seriously affect physical operations like transportation and the management

of large-scale networks like electric power. But even now major electric blackouts, or communications systems failures, are not unknown, and yet advanced countries manage to carry on. While the impact of cyber attacks may be hard to gauge in advance (see discussion below), the effect of disruptive cyber attacks is to throw sand into the gears.

For a rational player, the benefit of pure cyber attacks is in the demonstration of power, as in situations of escalating state-to-state tension or in limited war. Alternatively, cyber might be employed through proxy actors. In either case, though, its effectiveness as a stand-alone projection of power will be limited.

More attention needs to be given to the combination of cyber with physical attacks in any future conflict. For instance, occasionally major telecommunications blackouts in the US, including disruptions to civilian air traffic control, have occurred because a cable was accidentally dug up somewhere. If the intent were to disrupt select critical infrastructures, physical damage – like a dozen or so rented mechanical diggers, each accidentally cutting a cable on a select day – combined with cyber disruptions might be very effective. A physical attack could damage transmission nodes, for instance, while cyber attacks disrupt the damage assessment and response functions. Combined attack modes might be far more complex and difficult than single mode attacks to assess and prevent. Combined attacks might be particularly difficult to recover from if specialised equipment with few backups were destroyed; for instance, reportedly there are very few spare SS7 switches, the key switches in managing telecommunications backbones¹².

Importantly, NATO military systems rely heavily on information systems, many of which transport data over commercial networks. If a combined cyber-kinetic attack actually did succeed in disrupting commercial communications systems for hours or days, the potential to cripple military command and control (C2) systems might be a serious concern. Also, many weapons platforms rely on networked data transmissions, and these systems may have their own unique vulnerabilities to combined cyber-physical attacks.

Because of the limited impact of disruptive cyber attacks, cyber terrorism is probably an oxymoron. Cyber attacks conducted by terrorist organisations, for instance as criminal activities to finance their efforts, are likely in the future if not already taking place. Terrorist organisations routinely use the Internet for communications and other purposes just like any organisation. But disruptive cyber attack is not an effective means of inducing terror in target populations.

¹² SS7 stands for Signaling System no. 7, and is the name for the switches and supporting protocols that operate the major (trunk) telephone lines.

Even when, not if, terrorist organizations acquire the ability to launch sophisticated cyber attacks, these incidents largely will be shaped by the same considerations affecting state action. Most likely, terrorist attacks using cyber will also simultaneously employ kinetic means.

The Use of Cyber Power

Since everything associated with cyberspace is new – the very term “*cyber space*” dates back only to 1982 – not surprisingly *the use of cyber power* presents a number of challenges. Effective cyber power doctrine will have to address the following:

❖ *Technical attribution of the source of the attack is difficult*

Electrons do not bear national markings. Because the Internet’s creators never envisioned the need, the Internet has no reliable means for tracing where a message comes from. Furthermore, the Internet model was not designed to withstand malicious alteration of the transmission packets¹³; it is easy for attackers to forge the source address – the sender’s address – of a packet in a one-way communication. Usually network attack techniques employ a series of stepping stones, using compromised intermediate hosts to “*launder*” packets sent. These/packets can be changed in transmission hops between hosts, and so attempting to trace attacks by correlating similar packets will not work against a sophisticated attacker. Some of the best though inadequate means of attribution require “*hacking back*” through intermediate systems. A hack back may itself result in significant violations of the Law of War.

Therefore, the potential – perhaps great potential – exists for misattributing the source of cyber attack. This risk is compounded by the speed at which cyber power can be exercised.

There is no standard for how much evidence for the attribution of the attack is required for a particular type of response by the state attacked. The open question is whether a target state can lawfully act against the proximate or likely source of the attack, even though the target is by no means certain that the attack originated there.

Even if a nation acknowledges that an attack came from computers on its territory, the government could claim that the attack was from anonymous (or “*patriotic*”)

¹³ See also *footnote 1*. Each Internet packet has along with its small portion of the message an address header that directs the packet through intermediate to its final destination (think of a router as a postman sorting mail based on the packet’s address heading). The address header also contains the address of the sender; it is easy for a malicious hacker to alter this header information to make it appear that the message is actually coming from a different person, not the one who actually sent it.

citizens, as in the case of the Estonian and Georgian attacks, and the attacks against the US originating in China. The possible cooperation of non-state actors in a state-sponsored cyber attack further complicates attribution. Since the technical skills required for cyber attack are similar or equivalent to those of sophisticated cyber criminals and hackers, it may be that cyber attacks, though sanctioned or supported by the attacking state, use cyber criminal or hacker resources in part or whole. Hence, the challenge of attribution may extend not just to identifying the actual location of the cyber systems used in the attack but also to tracing the organisational linkages.

Alternatively, an attack could be traced back to a nation that claims that its systems were merely intermediate points from another state or actor, or unknowingly served as the launching point for a cyber attack. The circumstances in which lawful action can be taken by a target state against this intermediate nation are still being defined by legal experts and will be discussed later.

❖ ***The effects of a cyber attack can be highly uncertain or unexpected***

Since some attack tools, like worms and viruses, can spread globally, there is a real risk of collateral damage as these agents spread uncontrollably. The original worm, the Morris worm of November 1988, caused extensive damage to the nascent Internet, though that was certainly not the intent of its creator, a student from Cornell.

Also, cyber attacks seek directly to change the performance of highly complex cyber systems, which in turn may affect the behaviour of other highly complex physical systems like infrastructures. The behaviour of complex systems is, in general, not well understood; for instance, the actual causes of some widespread (accidental) electric power outages have never been satisfactorily explained. It seems likely that unanticipated system behaviour may cause outcomes other than those intended by the attacker.

Finally, cyber attackers may not know with certainty the extent to which the target has significantly improved its defences, or has back-up, perhaps non-cyber systems, to support critical functions.

These uncertainties can have serious implications. On legal and humanitarian grounds, unexpected collateral damage could be viewed as indiscriminate attack. If the unplanned impacts of a cyber attack include cutting off the target's command structure from component forces, then even more serious military and diplomatic problems could arise.

❖ ***For the target it may be difficult to distinguish intent***

If the target state sees only the technical details of a particular cyber attack, their decision-makers may find it almost impossible to determine whether the attack

was launched by a nation or by terrorists, criminals or vandals. Information from sources other than a technical analysis of what happened to the cyber systems attacked may be needed to attribute the source of the attack. Even if the source of the attack is known, it may be difficult to ascertain what the intent was. A passive attack, such as an act of cyber espionage, can have technical details very similar to an intentionally disruptive attack. Unlike physical attacks, the true damage resulting from a cyber attack may be difficult to assess quickly. The target decision makers may be uncertain of the “*true*” impact of the attack for a period of time, and therefore assume the worst until further information is available; if target decision-makers fear that the operational effectiveness of their command and control structure has been compromised, this period of uncertainty may be further extended. Although waiting “*to see*” what course an observed cyber intrusion takes may be the only effective way to determine its intended effect, waiting may not be a viable option for target decision makers who fear that a disruptive attack is underway.

Furthermore, some cyber attacks may have impacts that build up slowly and gradually, as in the case, for instance, of an attack against a financial system designed to corrupt data incrementally. The knowledge that such an attack has taken place presents the target decision makers with a potentially complicated set of choices about matters such as defence and response.

❖ ***Accidents can happen***

Even with proper command and controls in place, accidental cyber attacks can occur. As can happen when accidentally sending an e-mail, the wrong code could be relayed to a target; or a logic bomb or other software already implanted in the target system could be accidentally triggered by the network operators or a hacker.

❖ ***Threatening the “use of force” in cyber space can be problematic***

There may be a limited range of circumstances in which a threat to launch disruptive cyber attack will be regarded as credible by either the target state or the community of nations. A DDOS attack can be credibly threatened; there are no effective short-term defences, and the attack can be terminated at will. Cyber criminals routinely use the threat of DDOS attacks in extortion against online businesses. In other cases, however, the threatened use of cyber power, like the threat of force, which is prohibited by Article 2(4) of the UN Charter, may be less convincing. With exceptions like DDOS attacks, most disruptive cyber attacks are based on onetime use techniques, so that a demonstration attack may actually work to the detriment of the attacker. It seems therefore that the threatened use of cyber power will remain problematic. In other words, for diplomacy and cyber power to work in concert new ideas may have to be developed.

Consequently, deterrence in cyber space remains an undeveloped concept. The lessons of nuclear deterrence are not uniformly applicable to cyber power. Nuclear deterrence was based on a common understanding of the effects of nuclear devices and a certain confidence in the impact of promised deterrent actions. With cyber weapons, however, the same degree of confidence cannot be placed in their performance on demand. Furthermore, it is difficult to stage effective demonstrations of cyber power without reducing the very effectiveness of the cyber arsenal. Basing deterrence on other modes of response, e.g., kinetic responses, may further worsen a situation and certainly raises its own legal and diplomatic issues. Cyber space deterrence may thus have to rely on new formulations, just as nuclear deterrence evolved from concepts different from those common to conventional military power.

❖ ***Command structure and definition of combatants need clarification***

In the US at least, authority relating to the use of cyber power appears fragmented both across the national security community and between the government and private sector. The intelligence community uses tools very similar to those used by the military, but for very different purposes, and reports through different command structures. NATO appears to be addressing the challenges of cyber war in its forthcoming Strategic Concept, while in the US a sub-unified military cyber command has been created (see below). Nonetheless there remains some potential for multiple authorities to direct less than perfectly coordinated operations, particularly given the nascent state of cyber operations overall. Furthermore, in the US government, responsibility for cyber security is divided between the Departments of Defense (DOD) and Homeland Security (DHS).

Deciding whether and how to incorporate private sector-network management and control into a command structure may be even more challenging than coordination within governments and across Alliance members. Coordination across private networks and with the government depends on decisions made by civilian network managers of privately owned critical infrastructures. While better in some sectors, notably telecommunications, overall coordination is voluntary and seems haphazard.

A second major issue, affecting military, non-military government, and private sector networks alike, is the role of civilians in supporting or operating cyber systems used in disruptive cyber attack. In this context, the difference between combatants and non-combatants, traditionally fundamental in kinetic war, is far more nebulous. Given the principle of distinction, must the person who physically presses the “send” button launching a cyber attack be viewed as a combatant? It would be easy to envision circumstances in which major parts of actually performing

the functions of cyber power (e.g. software development, network management) were outsourced to the private sector, including international companies resident in NATO countries.

❖ **Cyber attack is a developing area under the law**¹⁴

A key question in the deployment of cyber power is under what circumstances a cyber attack or continuous series of cyber attack can constitute an armed attack, thus triggering the target states' right to respond forcefully through a legitimate exercise of self-defence. The Law of Armed Conflict provides the primary legal framework for understanding when it is legal for one nation to use force against another (*jus ad bellum*) and the rules that govern the behaviour of combatants who are engaged in armed conflict (*jus in bello*). In cyber attack, these considerations are important both for a target nation formulating appropriate and effective responses, and for the state contemplating cyber attack prior to the outbreak of hostilities but without intending to give cause for the outbreak of general hostilities.

The UN Charter prohibits a state from either threatening or using force against another state in the international community, excepting actions authorised by the Security Council, or acts of self-defence. Appropriate self-defence must reflect the principles of both "*necessity*" and "*proportionality*".

Legal scholars conclude that a considerable body of international law does apply to the use of force in cyber space. Some states, including the US, and the UN General Assembly have specifically identified cyber attacks as a threat to international peace and security. However, given their relative newness, there is no legal precedent as to how offensive cyber operations should be regarded. In defining when cyber attacks constitute a use of force, an "*effects-based approach*" focuses not so much on whether a cyber attack qua cyber attack constitutes a use of force, but whether a cyber attack with a specific effect constitutes a use of force. The US appears to have adopted this perspective. For example, in using this approach, a disruptive cyber attack on the financial system, significantly disrupting commerce, would result in damage to the state's economic well-being equated with an armed attack. A question is how to regard the placement, but not actual use, of logic bombs or other disruptive cyber attack software in target systems. Do these constitute hostile intent? Are they the cyber analogy of placing a large explosive device under a target military installation? Or are they more like "*sleepers agents*", as remembered from the Cold War?

¹⁴ For a much more detailed discussion, and many references, see "*Cybersecurity Symposium – National Leadership, Individual Responsibility*", *Journal of National Security Law and Policy* 4, no. 1, 2010. <http://jnslp.com/> (accessed 27 September 2010).

Three other issues relate to the definition of use of force. Although traditionally espionage has not been regarded as a use of force, there is some belief that cyber espionage, conducted over an extended time period and in large volume, as might be the case for the F-35 incident, constitutes a demonstration of hostile intent. Do such passive cyber attacks justify responses beyond taking additional passive defence measures? Such responses might include conducting counter-probes of the adversary networks from which the intrusions are originating, and even attacking these networks to neutralize the probes. These responses are sometimes called an “*active defence*”, and we will return to the implications of this approach when discussing NATO cyber defence policy. Finally, cyber operations affecting economic functions also fall into the ambiguities inherent in international law between the use of economic sanctions (which is legal), and blockades, which constitute an act of war.

A second set of questions relates to the nature of appropriate response and when can and should non-cyber responses (e.g. kinetic means) be employed in response to cyber attacks. This issue, relevant also to a concept of cyber space deterrence, remains unclear; there is to date no precedent. Such use might violate Law of War *jus ad bellum* considerations.

Also at issue legally is the perceived requirement that the target state must conclusively attribute a cyber attack to another state or its agents. Nations following this dictum historically have chosen to respond to cross-border cyber attacks as they would to criminal acts. However, in the case where a nation claims that non-state actors are at fault, over the past twenty years new thinking has emerged as to assigning state responsibility – as a sanctuary state – for the actions of non-state actors. Under the concept of “*indirect responsibility*” a state has an established duty to prevent its territory from being used as a launching pad for attacks. In the *International Law Commission’s Draft Articles on the Responsibility of States for Wrongful Acts* (2001), and as recognised by the UN General Assembly, the state is said to have breached its duty of responsibility when it consistently fails to undertake specifically identified measures designed to prevent attacks, such as the passage of legislation criminalising cyber attacks and the corresponding cooperation in investigation and prosecution of those engaging in cyber attacks. In that case, it becomes a sanctuary state and is vulnerable to a legitimate use of force by the victim state.

NATO and US Posture Re Cyber War

❖ **NATO**

NATO documents usually reference cyber defence rather than cyber war or cyber power. Operationally, NATO cyber defence activities are centred in three groups:

- *The NATO Computer Incident Response Capability (NCIRC)*, created in 2002, handles and reports cyber security incidents and disseminates important incident-related information to systems/security management and users. NCIRC is part of the NATO Communications and Information Services Agency.

- *The Cooperative Cyber Defence Centre of Excellence (CCDCOE)* was established in 2003, and accredited as a NATO Centre of Excellence (COE) in 2008. It conducts research and training on cyber warfare. Currently sponsoring Alliance members are Estonia, Germany, Italy, Latvia, Lithuania, Slovakia, and Spain, with the US, Turkey, and Hungary joining. Its activities are also supported by the *NATO Science Programme*.

- *The Cyber Defence Management Authority (CDMA)* has sole responsibility for coordinating cyber defence across the Alliance. CDMA is overseen by the *NATO Consultation, Control and Command (NC3) Board*. Also, in August 2010 the *Emerging Security Challenges Division (ESCD)* was created within the NATO International Staff to address non-traditional risks and challenges, including cyber defence.

NATO's attention to cyber defence dates back at least to 2002, when implementation of a Cyber Defence Programme – “*a comprehensive plan to improve the Alliance's ability to defend against cyber attacks by improving NATO's capabilities*” – was approved by the North Atlantic Council¹⁵. This Programme also supports the *Prague Capabilities Commitment (June 2002)*, which identified deployable and secure command, control and communications as one of eight fields for improvement. Further commitments to the Cyber Defence Programme were made in the *2006 Comprehensive Political Guidance* and at the 2006 Riga Summit.

The cyber attacks on Estonia in April-May 2007 transformed the scope of NATO cyber defence activities. Prior to then, NATO efforts were primarily concentrated on protecting the communications systems owned and operated by the Alliance. During the DDOS attacks against Estonia, responding to a historic request by a NATO member in defence of its digital assets, NATO members, including the US, provided technical assistance. As a result of the Estonian attacks, NATO has developed more formal guidance for supporting Allied nations if they need

¹⁵ NATO, “*Defending against Cyber Attacks*”, www.nato.int/cps/en/natolive/topics^491_93.htm?selectedLocale=en (accessed 27 September 2010). Unless noted, material in this and following paragraphs is drawn from this report.

to counter cyber attacks. *“This implies that NATO has developed mechanisms for assisting those Allies who seek NATO support ... including through the dispatch of Rapid Reinforcement Teams”* – although, as will be discussed shortly, further work in this area appears to be needed. In parallel, supporting refinements or new initiatives have been made in three areas: NATO cyber defence policy, NATO cyber defence military concept, and measures to accelerate the hardening of NATO’s own information systems against cyber attack.

“Practical cooperation on cyber defence” with NATO partners is being developed in accordance with the *“Council Guidelines for Cooperation on Cyber Defence with Partners and International Organisations”* (August 2008) and the *“Framework for Cooperation on Cyber Defence between NATO and Partner Countries”* (April 2009). Estonia, Slovakia, Turkey, the UK and the US have signed agreements with NATO to facilitate cooperation in the event of a cyber attack¹⁶.

[NATO is now in the process of updating the NATO Strategic Concept, last revised in 1999]. The language of the Group of Experts’ Report informing this process may suggest elements of NATO’s new cyber defence posture¹⁷:

The threat: *“The most probable threat to Allies in the coming decade are unconventional ... The next significant attack on the Alliance may well come down a fiber optic cable”*.

The gap: *“...there persist serious gaps in NATO’s cyber defence capabilities. The Strategic Concept should place a high priority on addressing these vulnerabilities, which are both unacceptable and increasingly dangerous”*.

The need: *“The danger posed by unconventional threats has obvious implications for NATO preparedness, including its definition of security, its strategies for deterrence, its need for military transformation, its ability to make decisions rapidly, and its reliance for help on countries and organisations from outside the Alliance”*.

The recommendations: *“NATO must accelerate efforts to respond to the dangers of cyber attacks by protecting its own communications and command systems, helping Allies to improve their ability to prevent and recover from attacks, and developing an array of cyber defence capabilities aimed at effective detection and deterrence”*.

The Report recommends that *“to guard against these threats [including cyber attacks], which may or may not reach the level of an Article 5 attack, NATO must update its approach to the defence of Alliance territory while also enhancing its ability to prevail in military operations and broader security missions beyond its borders”*.

¹⁶ NATO Newsroom, *“Interview with NATO Assistant Secretary General for Defence Investment Peter Flory”*, 28 March 2008, www.nato.int/cps/en/natolive/opinions_7598.html (accessed 27 September 2010).

¹⁷ NATO, *“NATO 2020: Assured Security, Dynamic Engagement; Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO”*, 17 May 2010, www.nato.int/cps/en/SID=F9F9C7EC-4E74993B/natolive/official_texts_63654.htm?selectedLocale=en (accessed 27 September 2010). Unless noted, material in this and following paragraphs is from this source.

The Group of Experts report further specifically recommends five actions:

- Increase the monitoring of NATO's critical network and assess and furnish remedies to any vulnerabilities that are identified.
- The CCDCOE should do more, through training, to help members improve their cyber defence programs.
- Allies should expand early warning capabilities in the form of a NATO-wide network of monitoring nodes and networks.
- The Alliance should be prepared to send an expert team to any member experiencing or threatened by a major cyber attack.
- Over time, NATO should plan to mount a fully adequate array of cyber defence capabilities, including passive and active elements (*italics added*).

These recommendations raise at least two challenging issues for NATO doctrine. Active cyber defence is a somewhat nebulous term of art. While passive defence includes commonly used practices such as firewalls, virus protection and network monitoring – steps taken by any responsible organisation – active defence can include practices such as aggressive efforts to trace the source of incoming cyber attacks, or actions to disable the attack source. Active defence as a component of NATO doctrine will require careful definition. Such a definition is made even more challenging given the dynamic technological changes ever-present in the nature of cyber attack and defence.

It is also unclear on what Treaty basis NATO would act in the event of a cyber attack or threat of cyber attack against any member – Article 4 or Article 5 of the North Atlantic Treaty?¹⁸ *“The Group of Experts’ Report notes that Article 4 consultations are «singularly well-suited to the review of unconventional dangers ...».* However, *“there may well be doubts about whether an unconventional danger – such as a cyber attack ... – triggers the collective mechanism of Article 5”.*

❖ ***The United States***

In the US, since 1998, when Presidential Decision Directive 56 called for a national policy to protect critical infrastructures, particularly cyber-based, defensive postures, cyber security has been the focus of continued government and private sector attention. In 2008, at the beginning of the Obama Administration,

¹⁸ In the 1949 North Atlantic Treaty, Article 4: *“The Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence, or security of any of the Parties is threatened.”*; Article 5: *“The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all”.* www.nato.int/cps/en/natolive/officialtexts_17120.htm (accessed 27 September 2010).

a quasi-official report noted that “*The United States must treat cybersecurity as one of the most important national security challenges it faces ... This is a strategic issue on par with weapons of mass destruction and global jihad*”¹⁹.

It is important to note that the US perceives itself as having a greater vulnerability to cyber attack than other nations, for several reasons. The US has a greater dependency on cyber-controlled systems than potential adversary nations. Few nations, and certainly no US adversaries, have more essential national systems in private hands; furthermore, cyber security for critical infrastructures is largely voluntary, and it is unclear how robust these infrastructures would be in the face of a sophisticated disruptive cyber attack. Finally, the US military perceives itself as being highly vulnerable to cyber attack. As noted by Defense Secretary Gates, “*With cheap technology and minimal investment, current and potential adversaries operating in cyberspace can inflict serious damage to DOD’s vast information grid...*”²⁰.

US defensive cyber policy is some ways dysfunctional. The two lead government agencies tasked to defend the United States are the DOD, responsible for defending national security systems, and the DHS, responsible for defending, in “*public-private partnership*”, the eighteen designated critical infrastructures as well as other non-national security assets. A White House official, reporting both to the National Security Advisor and to the National Economic Advisor, is responsible for overall policy coordination. Under the 2003 “*National Strategy to Secure Cyberspace*”, US policy has been to eschew regulations or mandates on privately owned critical infrastructures, including telecommunications and most facets of cyberspace, in favour of self-directed plans for protection, information sharing and response.

But beyond efforts to protect themselves against cyber crime, it is unclear how much the private sector is concerned (or should be concerned, on a voluntary basis) in defence against national-level cyber threats. Few, if any, observers regard this system as providing adequate direction or incentive for a national cyber defensive posture, if indeed this is possible. Defence of national security systems, however, has been a longstanding priority of the Defense Department. Use of national security assets to defend civilian cyber space is problematic; while reportedly the Defense Department has considered such a role, the *DOD’s National*

¹⁹ James A. Lewis et al, “*Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency*”, Washington, Center for Strategic and International Studies, 2008, p. 15, http://csis.org/files/media/csis/pubs/081208_securingcyberspace-44.pdf (accessed 27 September 2010).

²⁰ Secretary of Defense Robert M. Gates, “*Submitted Statement to the Senate Armed Services Committee*”, Washington, US Senate, 27 January 2009, http://armed-services.senate.gov/statement/2009/January/Gates_01-27-09.pdf, (accessed 27 September 2010).

Security Agency (NSA), which has primary responsibility for supporting DOD's cyber security duties, is not authorised to assist private sector critical infrastructure systems directly²¹.

More recently, cyber war, and implicitly the concept of cyber power, have received much attention in America. However, US offensive (disruptive cyber attack) policy and doctrine is inchoate at the present. In 2002, National Security Presidential Directive 16 called for a national policy on the rules of engagement for using cyber warfare as a weapon. A 2006 DOD Directive assigned baseline responsibilities for the conduct of "information operations". In the *2009 Quadrennial Roles and Mission Review* Secretary Gates designated cyber space as one of the four focus areas, a reinforcement of tenets in the 2005 and 2008 National Defense Strategy. A recent commentator notes that the DOD strategy "is to establish the foundation for developing capable cyber forces; structure the forces, as well as their processes and procedures; and then employ these forces to achieve desired effects across the full range of military operations"²².

The *US Cyber Command (USCYBERCOM)* is now standing up, with an initial operating capability scheduled for November 2009 now delayed. USCYBERCOM is a subunified command under the *US Strategic Command (USSTRATCOM)*. USSTRATCOM is tasked under the Unified Command Plan to direct the defence of the Global Information Grid and synchronise cyberspace operations. However, a number of observers are critical of the current state of US policy and coordination; as one notes, the US "has a military Cyber Command but not a cyber war strategy, not a major policy or program to defend the private sector, nothing to initiate international dialogue on cyber war"²³. A close reading of the news suggests that there are numerous rivalries among the DHS, NSA and various other parts of the DOD over who controls what within the domains of cyber security and cyber war, with the US Congress weighing in with various proposed bills now under consideration.

The US is already engaged in bilateral discussions concerning military use of cyber space. Russia supports forging an international treaty banning countries from engaging in cyber war, similar to past chemical warfare negotiations, and has made proposals for such a treaty in the United Nations. The US in turn has advocated improved cooperation among law enforcement agencies, the starting framework for which is already provided by the *Council of Europe Cybercrime Convention*, which the US has ratified, though many Alliance members have not.

²¹ Some thought has been given to DOD defense of civilian networks; Ellen Nakashima, "Cyber-Command May Help Protect Civilian Networks", *The Washington Post*, 5 May, 2009.

²² Jeffrey Caton, "What Do Senior Leaders Need to Know about Cyberspace?" in *Crosscutting Issues in International Transformation: Interactions and Innovations among People, Organizations, Processes and Technology*, ed. by Derik Neal et al, Washington, National Defense University, December 2009, p. 207.

²³ Clarke, p. 118.

An Agenda for the Future

Concerns about growing security threats in cyber space are valid. These concerns are grounded on the combination of growing national dependence on cyber systems, and the pervasive vulnerabilities in these systems.

Cyber attacks, both passive and disruptive, exploit these vulnerabilities; both criminals and nation states have effectively employed cyber attacks of both types. While some of these attacks have been called examples of cyber war, I believe that the term “*cyber war*” is misleading. To draw an analogy from naval thinking, since the writings of Alfred Mahan²⁴ sea power rather than naval war has been the preferred strategic frame of reference for the projection of state power on the oceans. Like “*naval war*”, cyber war conjures up legal, policy, military, and diplomatic considerations that inappropriately narrow the scope of relevant issues. Cyber space is better thought of as a new theatre for states to exercise cyber power and not just to conduct cyber war. In nuanced ways perhaps not yet seen, cyber power can involve both the projection of state power as well as the creative use of active defences, all in concert with other military, diplomatic, information and economic tools. The projection of cyber power with both offensive and defensive elements must be a component of national and NATO security doctrine for the future.

The effective exercise of cyber power by NATO presents a number of new issues, including defining when a cyber attack constitutes the use of force, developing a theory of deterrence in cyber space, and clarifying the role of civilians operating cyber systems in a cyber conflict. A special issue for NATO will be to select the appropriate framework for providing assistance to Partners threatened by cyber attack. Should Article 4 be invoked, or Article 5 ? Furthermore, while NATO has made substantial progress in defining a cyber defence posture, it is clear that serious gaps in capability and doctrine remain. The forthcoming NATO Strategic Concept provides an opportunity for addressing these concerns.

In the future, disruptive cyber attacks launched by states will occur. Almost certainly we will see again what has already occurred – cyber attacks against significant civilian, government, and military systems of Alliance members without clear technical attribution of the source of the attacks. The likely attacker will claim plausible deniability. Effective means of defending against prolonged attacks will prove difficult, or an accidental disruptive cyber attack might occur. However, absent non-rational actors, I find it difficult to envision disruptive cyber attacks without kinetic accompaniment in any context other than limited warfare,

²⁴ Alfred Thayer Mahan, *The Influence of Sea Power Upon History 1660-1783*, Twelfth Edition, Boston, Little, Brown and Company, 1890.

escalations prior to the outbreak of hostilities, or accidents. An attempt at full-scale cyber war without kinetic attacks does not appear to make sense. While serious, the scope of damage from cyber attack is inherently limited compared with that achievable by conventional means. Over anything more than a short period of time (weeks or months) the effectiveness of cyber attacks likely will decline as alternatives to vulnerable systems are deployed or as cyber systems are hardened and therefore made less vulnerable.

Disruptive cyber attacks by terrorists are possible, even likely, but cyber qua cyber is not a weapon of terror. Cyber attacks could be viewed as a weapon of mass annoyance. Clearly, while cyber threats from non-state actors are not addressed in the same way as attacks from hostile states, the framework of issues shaping NATO doctrine and policy should for the most part be the same.

Given this future, there is need for the NATO alliance to develop a clear doctrine of cyber power, addressing issues of offensive use, defence, response and deterrence. This article has outlined key issues which doctrine must address.

Supporting foreign policy must accompany this doctrine²⁵. Specifically, there is a need for an agenda to at least consider the development of bilateral and multilateral frameworks for defining the justification for and form of military action in cyber space, mediation of cyber conflicts and limitations on the exercise of cyber power. Given the complexities and newness of cyber attack as a tool for nations, it is unlikely that a nation seeking UN redress would see rapid action. NATO must be prepared to act.

Proposals for a cyber arms control regime are likely to be part of the future. Russia appears intent on pursuing this agenda. The development of arms control protocols is usually a long and complex process. The key point is that the foreign policy of NATO members should be consistent with the NATO doctrine of cyber power, and mutually supportive across member nations of agreed goals.

NATO doctrine for cyber war and cyber power will continue to evolve – rapid technological change alone ensures that. Cyber space represents a new environment for the projection of power – cyber power – and NATO needs to address this challenge on an on-going and committed basis.

²⁵ Jeffrey Hunker, “US International Policy for Cybersecurity: Five Issues That Won’t Go Away”, *Journal of National Security Law and Policy* 4, no. 1, 2010. <http://jnslp.com> (accessed 27 September 2010).

MULTI-RESOLUTION FEDERATIONS IN SUPPORT OF OPERATIONAL AND HIGHER LEVEL COMBINED/JOINT COMPUTER ASSISTED EXERCISES

Dr Erdal CAYIRCI

Multi-resolution federations are still in their infancy. Their usefulness is often discussed and there is confusion about the related taxonomy. In this paper, first the definitions for the field are clarified, and the latest developments are explained. Then the advantages of multi-resolution federations in support of computer-assisted exercises are explained by using an example vignette.

Keywords: *military simulation; constructive simulation; combat models; multi-resolution federations, joint theatre level simulation, joint conflict and tactical simulation, virtual battle simulation, computer-assisted exercise.*

In the military, simulation is used for various purposes, such as capability development, defence planning, operation support and training. Simulation justifies itself, perhaps the best for the military, because it considerably reduces the cost of these functions. Simulation is also the only way to test and train for some special environments, such as nuclear, biological and chemical contamination and operations that require large-scale mobilisation and movement. Creating and maintaining such environments are simply impractical in real life without interfering with natural life. These hostile environments also imply casualty risks. Therefore, simulation is not only a cost-effective approach for military but also the only practical and safe way for testing and training for special and hazardous situations. Therefore, military simulation systems¹ have been used extensively.

Dr Erdal Cayirci – CAX Support Branch, NATO Joint Warfare Center, Stavanger, Norway.

¹E. Cayirci, D. Marincic, *Computer Assisted Exercises and Training: A Reference Guide*, Wiley & Sons, 2009; J. R. Surdu and U. W. Poach, *Simulations Technologies in the Mission Operational Environment*, *SCS Simulation*, vol. 74, no. 3, March 2000, pp. 138-160.

They can be categorised into three broad classes shown in *table 1*².

Category	People	Systems
Live	Real	Real
Virtual	Real	Simulated
Constructive	Simulated	Simulated

Table 1: Military simulations

> *Live simulation* refers to a simulation that involves real people operating real systems. For example, two pilots can be trained for dog fighting by using real aircraft in the air. In this case, the aircraft and the pilots are real, but the interactions between the aircraft are simulated and the simulation decides how effective the pilots and the aircraft are against each other. Similarly, all the weapon systems can be equipped with emitters and all the equipment and personnel can be equipped with sensors. If the weapons are aimed and fired correctly, the emission by the emitters can be sensed by the sensors, which indicates a hit and a kill based on some stochastic processes.

> *Virtual simulation* refers to a simulation that involves real people operating simulated systems. Examples for this are aircraft and tank simulators, where a simulator but not a real system is used to train a pilot or tank crew.

> *Constructive simulation* refers to a simulation that involves simulated people operating in simulated environments. Combat models that compute the possible outcomes of the decisions taken by headquarters fall in this category. In these simulations, people and units are also simulated, as well as combat systems and environment. Although the interaction of these categories of simulation systems is possible by using the state-of-the-art technology, and all of them, i.e. live, virtual and constructive simulations may be used during the execution of a *computer-assisted exercise (CAX)*, a military constructive simulation system constitutes the core of a CAX. The definition of constructive simulation states that the people operating the simulated systems are also simulated. However, real people enter the commands to stimulate these simulations. Constructive simulations are designed to find out the possible outcomes of the courses of actions taken by the real people. They are constructed by many models often stochastic processes that calculate the results of interactions between the entities or units in a theatre. Constructive simulation systems can be classified into two categories according to their resolution as summarised in *table 2*:

Category	Level	Objects	Terrain
High Resolution	Entity	Singular objects, e.g. a tank, a troop	High resolution, 200 x 200 km
Highly Aggregated	Aggregate	Units, e.g. a battalion, a company	Low resolution, 4 000 x 4 000 km

Table 2: Military constructive simulations

² E. Cayirci, *NATO Joint Warfare Center's Perspective on CAX Support Tools and Requirements*, ITEC'2006, May 2006.

➤ *High-resolution simulations* are *entity level simulations* where singular military objects, e.g. soldiers, tanks, aircraft, are the primary objects represented. The resolution of terrain data is high sometimes up to the plans of individual buildings. However, the simulated terrain is often limited to 200 km x 200 km. High-resolution simulations better suit for tactical level. However, they are not only for tactical level simulation. They provide higher resolution that may be required also for operational and higher level purposes. Therefore, high-resolution simulation systems should not be called as tactical simulations.

➤ *Highly aggregated simulations* are aggregate level simulations where collections of military assets, i.e. units, are the primary objects represented. They use lower resolution terrain data but they can simulate in very large areas as large as continents. Similar to high-resolution simulations, there is a tendency to call highly aggregated simulations as operational level simulations, which is not correct. Aggregate level simulations may be very useful also for tactical purposes. Please note that, in civilian content, tactical level is over operational level, which is opposite to the military hierarchy. In this paper, we use the military hierarchy in our definitions.

The gap between high resolution and highly aggregated simulation systems tends to be narrowed. State-of-the-art entity level simulations can be used for simulating operations in regions as large as 2 500 km x 2 500 km. On the other hand, aggregate level simulations tend to be capable to simulate the entities such as a single troop and a tank. However, the nature of CAXs in operational and tactical levels requires the assessment of the situation in aggregate and entity levels respectively, and the CAXs are manned according to this, though it may sometimes be required to interact with the simulation in multiple levels. Therefore, the current trend is toward having either a single system that can aggregate and de-aggregate³ the units and entities or a multi-resolution federation of entity and aggregate level simulations.

The constructive simulation systems can also be categorised based on their functionalities as follows:

- *Service models* are the simulation systems developed for the needs of a single service, i.e. army, navy or air force.
- *Joint models* are either simulation systems that fulfil the requirements of all services or federations made up of service models.
- *Expert models* are developed specifically to simulate certain functionalities such as logistics, intelligence, electronic warfare, homeland security and space operations.

³ P. F. Reynolds, S. Srinivasan, *Consistency Maintenance in Multiresolution Simulations*, ACM Transactions on Modeling and Computer Simulation, vol. 7, no. 3, pp. 368-392, July 1997.

In this paper, we examine the usefulness and practicality of multi-resolution federations⁴ that integrate all these classes of constructive simulations, as well as live and virtual simulations into a seamless simulation environment through distributed simulation technologies, mainly *high level architecture (HLA)*⁵. We aim:

- to provide a *tutorial* on CAX and how computer simulations are used in a CAX.
- to provide a *tutorial* on multi-resolution constructive simulation federations, which is an emerging technology for the military application of distributed computer simulations.
- to explain the importance of multi-resolution federations for combined/joint exercises in operational and higher levels.

In Section 2, we elaborate on a CAX architecture, which is typically made up of two main components, training audience (TA) and exercise control (EXCON). In the same section, we explain why constructive simulation systems are used and who uses them in a CAX. In Section 3, multi-resolution federations and NATO Training Federation (NTF) are introduced. Then an example for incidents that require high-resolution modeling even when they are practiced by operational and higher level headquarters are examined in Section 4. We conclude our paper in Section 5.

Training Audience, Exercise Control, Response Cells and Simulation

A CAX is set up based on TA and training objectives⁶. Throughout the CAX process, from the start of exercise specification until the end of *after action review (AAR)*, these two should always be the focus. A TA can be single level, multi-level, cross-level and both cross- and multi-level as shown in *figure 1*.

Multi-level training audience represent multiple levels of command trained at the same time in the context of a single scenario. Cross-level TA includes units or headquarters at the same level of command. When the units in a cross level TA

⁴ A. Bowers, *Multi-Resolution Modeling in the JTLS/CATS Federation*, Technical Report, MITRE Cooperation, 2003.

⁵ IEEE, *IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA) – Framework and Rules*, Std 1516, 2000; IEEE, *IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA) – Federate Interface Specification*, Std 1516.1, 2000; IEEE, *IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA) – Object Model Template (OMT)*, Std 1516.2, 2000; Defense Modeling and Simulation Office (DMSO), *High Level Architecture Interface Specification*, Version 1.3NG, Washington DC, 1998.

⁶ E. Cayirci, D. Marincic, *Computer Assisted Exercises and Training: A Reference Guide*, *op. cit.*; E. Cayirci, *Exercise Structure for Distributed Multi-resolution NATO Computer Assisted Exercises*, ITEC'2007, May 2007.

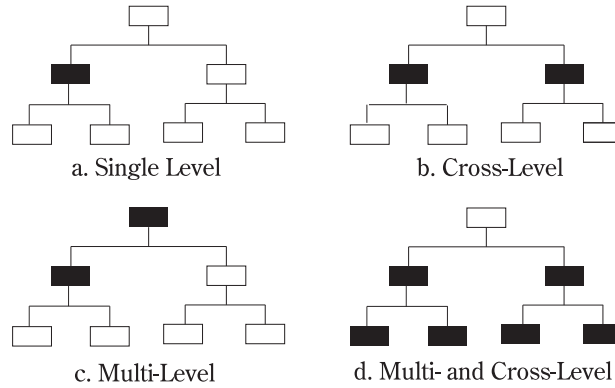


Figure 1: Training audience

are from different services, the exercise becomes a *joint exercise*. A TA can have forces from different nations, which makes the exercise *combined*. In more and more exercises, civilian national/international agencies and organisations like police, fire department, health agencies and UN are involved in. Most of the time, these civilian organisations become a part of EXCON and constitute a *white cell*. They may also be a part of TA.

TA can be co-located or various parts of TA can be located in geographically remote sites, i.e. different cities, countries, continents etc. The exercises that have TA components located in *remote sites* are called *distributed exercises*. Please note that distributed simulation and distributed exercise are different things. A distributed exercise can be supported by a centralised simulation system or a centralised exercise can be supported by distributed simulation. Locating terminal workstations of a simulation in remote sites does not make a simulation distributed. In distributed simulation, computation for the simulations is carried out by multiple processes often in remote machines.

The second component of a CAX is EXCON. A typical EXCON model is shown in figure 2. *Training team (TT)* consists of *mentors, observer/trainers (O/T), subject mater experts (SME)* and *analysts*. TT is deployed with TA,

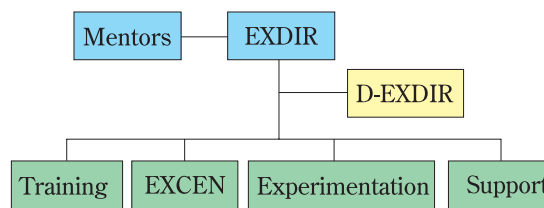


Figure 2: EXCON Structure

observe TA, provide on site instructions and training, and collects inputs for AAR and the evaluation of TA. *Exercise center (EXCEN)* is the organisation responsible for the consistent and coherent flow of the exercise according to the exercise objectives. EXCEN is explained in detail below. Experimentation team runs the experiments planned in conjunction with the exercise. Finally, support team

has the elements like *real life support (RLS)*, *visitor officer bureau (VOB)*, *public information centre (PIC)*, *security office* and *computers/communications support team*.

EXCEN functions (figure 3) can be categorised into five broad classes as *situation centre (SITCEN)*, *higher control (HICON)*, *lower control (LOCON)*, *white cell* and *situation forces (SITFOR)*. SITCEN monitors the status

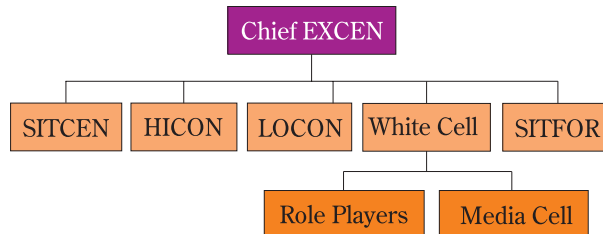


Figure 3: EXCEN model

of the exercise closely and steers it according to the training objectives. HICON and LOCON represent the command levels/echelons that would normally be at the level above and below the TA respectively. White cell is a response cell that is composed of subject matter experts (SME) or role players representing agencies, organisations, institutions and individuals outside of the own or opposing force structure. SITFOR is the cell that manages the status of all the own and opposing forces in the scenario except for the ones represented by HICON and LOCON. When opposing side is also played by a part of the TA, only the parts of forces not controlled by the TA are managed by SITFOR.

One of the teams in SITCEN (figure 4) is the scenario team, which is responsible to maintain and manage the scenario related information, and to respond the *requests for information (RFI)*.

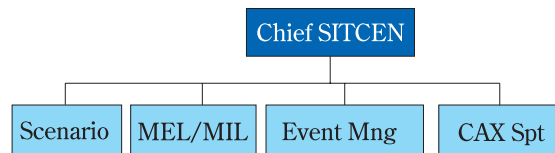


Figure 4: SITCEN model

They have a close connection and coordination with the SITFOR cell.

Main Event List (MEL)/Main Incident List (MIL) team is another important team within SITCEN. In order to achieve the exercise objectives, events and incidents are designed and injections are developed according to them before the exercise. “Events are major occurrences or a sequence of related incidents, which are actions or situations that provide greater clarity to an event. An injection is the way of bringing an incident to the attention of players”. MEL/MIL is not fixed, and should be modified during an exercise, i.e. dynamically scripted throughout the exercise. MEL/MIL manager closely monitors the status of every injection, and manages dynamic scripting and timings of injections. MEL/MIL team ensures that every injection serves for a *training objective (TO)*, the coverage of TA, TO and the exercise duration by the injections are very well balanced.

Event managers manage the main events from start to end. They ensure that the TO for the event are achieved by the TA. They closely follow the feedback from O/Ts and *response cells (RC)*, design new incidents consistent with the scenario, simulation, the overall event and TO, and ensure that the planned incidents are injected at the correct time, i.e. consistent with the scenario and status, to the targeted TA. They coordinate with the subject matter experts (SME) in functional desks, CAX support team and MEL/MIL manager. CAX support team in SITCEN provides the interface between the simulation operators and SITCEN. LOCON and HICON consist of RC. The number of RC is dependent on the scenario and the TA. Each RC is made up of a MEL/MIL coordinator, a number of planners and a number of simulation operators. RCs are the main interface between simulation and exercise. The interaction between simulation systems and TA during a CAX is depicted in *figure 5*. There are two ways

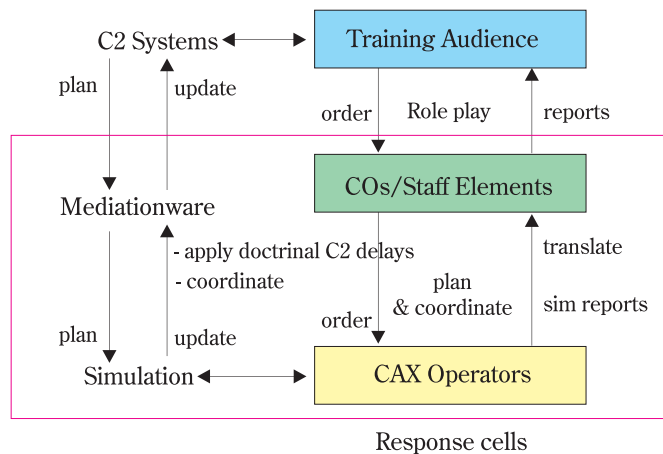


Figure 5: Simulation and the training audience

for this and both of them are indirect for TA. The first way is through the response cells who are acting as LOCON to the TA. TA gives an order and a response cell role plays as the subordinate unit headquarter that receives the order. Then, the planners in the response cell coordinate and plan the execution of the order, and after applying some doctrinal C2 delays, they pass the plans to the CAX operators who translate them to the simulation orders. CAX operators receive both periodical and mission reports from the simulation system. They translate these reports to the planners in the response cell, who role play to pass the reports to the TA. This interaction with the simulation system is through the *role play* by the response cell.

The second way is automatic interaction through *command and control (C2)* systems. Simulation systems can interact automatically with the operational C2 systems

of TA by using *mediation-ware*. For example, the *air tasking orders* developed in a C2 system can be translated into the simulation orders and directly fed into the simulation. This interaction is from the C2 system to the simulation. The opposite direction is also possible. For example, the simulated air missions can update the recognised air picture in C2 device automatically and continuously.

The bottom line is that RCs are the main component which directly interacts with simulations in a CAX. In this construct, simulation is used for the following reasons:

- *reason 1*: to compute the possible outcomes, i.e. results of the decisions made by TA.
- *reason 2*: to simulate the entities and conditions not controlled by the TA or EXCON.
- *reason 3*: to maintain a consistent white truth. Recognised operational pictures are derived from the white truth according to the intelligence capabilities and efforts of the sides and services.
- *reason 4*: to stimulate Command and Control (C2) systems used by TA.

All these reasons are important. Although simulation systems are designed mainly for the first two reasons, they can be used only for the last two in totally scripted exercises, i.e. exercises where the plans of TA are not simulated, but the results of their decisions are prescript based on forecasting, and modified during the exercise according to the developing situation based on intuition. This is called *dynamic scripting*. Of course, when TA is given injections based on experience and intuition of EXCON, the risk that the injections are not coherent and realistic is higher. We call this risk as “*negative training*” risk because a headquarters trained with unrealistic injections may plan considering that they can achieve the same results also in a real battlefield. Therefore, we believe that verified and validated simulation systems with validated databases are important and can reduce the “*negative training*” risk. Realism that a simulation can provide is related to its capabilities. Multi-resolution federations concept is a both time and cost effective way to achieve constructive simulation environments with enhanced simulation capabilities.

Multi-resolution Federations and NATO Training Federation

Multi-resolution federations are federations that integrate highly aggregated and high-resolution simulations into a distributed simulation system typically by using HLA. Virtual and live simulation systems can also become federates in a multi-resolution federation. Therefore, there is not necessary to differentiate

multi-resolution federations from live virtual constructive (LVC) federations. However, this differentiation is often made, i.e. LVC federations and multi-resolution federations are often built separately. There are two main reasons for this:

- Virtual and live simulations have to be real time. On the other hand, being able to run faster or slower than real time is a desirable feature for constructive simulations.
- Many virtual and live simulations are already federated by using the *Distributed Interactive Simulation – DIS*. There is a *federation object model (FOM)* called *real-time platform reference (RPR)*, FOM designed, based on *DIS protocol data units (PDU)*. Therefore, many LVC federations use RPR2 FOM. Since the latest RPR FOM does not support entity-aggregate interactions, it is not preferred for multi-resolution federations. Modular FOM approach in *HLA 1516-Evolved* provides new techniques to create a modular FOM that can include both RPR and other modules more appropriate for multi-resolution federations. There is already work to create reference architectures that can be used as both LVC and multi-resolution federations. However, most of the current multi-resolution federations are designed and implemented separately from LVC federations. Some examples for these implementations are *multi-resolution federation (MRF)* and *joint multi-resolution model (JMRF)* in the US, *partnership for peace simulation network (P2SN)* reference architecture by NATO partner nations, *KORA* and *SIRA* federation (*KOSI*) in Germany, and *ALLIANCE* in France. Most of these federations are still maturing, and not used in a major exercise.

NATO training federation (NTF) is a multi-resolution HLA federation derived from JMRF, and successfully used in a major NATO exercise first time in 2008 (figure 6). Initial NTF has two combat models, namely joint theatre level simulation (JTLS)⁷ and joint conflict and tactical simulation (JCATS). JTLS is a joint highly aggregated constructive simulation system. It best fits when the simulated units (simulation entities) are battalions, wings/air packages, i.e. multiple aircrafts in an air mission, and ships (frigates, submarines etc.) JCATS is a joint high-resolution constructive simulation, where the details like a single troop can be simulated by using high-resolution terrain and environmental data.

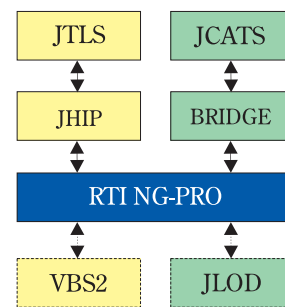


Figure 6: NATO Training Federation

⁷ E. Cayirci, C. Ersoy, *Simulation of Tactical Communications Systems by Inferring Detailed Data from the Joint Theater Level Computer Aided Exercises*, *SCS Simulation Journal*, 78, 475-484(2002).

It is also possible to aggregate the simulated entities into units and command them as aggregated units in JCATS.

Currently Virtual Battle Simulation (VBS2) is also federated with JCATS through distributed interactive simulation (DIS, IEEE 1278). Making VBS2 also an HLA federate to NTF is within the plans. Similar to VBS2, JCATS Low Overhead Driver (JLOD) is also within the area of interest for NTF. JLOD can complete NTF with non-kinetic warfare and civilian traffic simulation capabilities.

NTF is a very good example for reusability and interoperability of simulation tools. When the training audience is lower than or equal to component command (corps) level, JCATS provides better fidelity simulation.

On the other hand, since it is high resolution, it needs many details for operating. Therefore, it is not viable to use purely JCATS in exercises where high number of units and large areas are involved, e.g. corps and higher-level exercises. JTLS is a very good match for those levels. However, many incidents of contemporary warfare and conflicts require high resolution planning also in high echelons, which is not available in JTLS. NTF connects JTLS and JCATS to close this gap. In NTF highly aggregated JTLS can be used as long as higher resolution simulation is not needed. When simulation resolution higher than the one that JTLS can provide is required, JCATS can be used. The outputs of these two simulations update the attributes of the units and entities in both simulations. C2 systems can be stimulated by one of the federates in NTF, i.e. JCATS or JTLS, or become a federate themselves.

When NTF is available, some entities are simulated by JCATS, and some units in the same theatre are simulated by JTLS. The entities in JCATS are able to interact with the units in JTLS, which means an aircraft in JCATS can fire a missile to a ship in JTLS. This creates a new question to answer: "Which entities or units should be simulated in JTLS or JCATS?" The ownership of simulated objects can also be switched between JTLS and JCATS from time to time. The mapping between the simulation requirements and simulation systems can be based on the following criteria⁸:

➤ *geography based sharing of the units and entities*: The entities can be shared between multiple simulation systems based on geography. As shown in figure 7, we can give the simulation responsibility of a certain area to JCATS, while the responsibility for all the other regions stays with JTLS. The JCATS may also

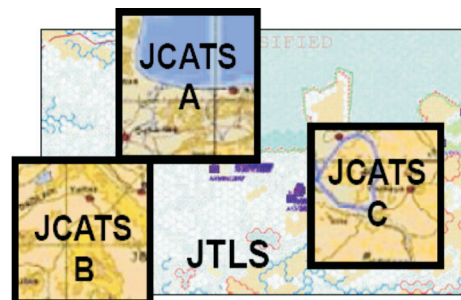


Figure 7: Geography based ownership

⁸ E. Cayirci, *Distributed Multi-resolution Computer Assisted Exercises*, NATO Modelling and Simulation Conference, October 2007.

have multiple geographic regions and change the areas from time to time. For example, Region A can be in JCATS at the beginning for a while, and then it may be returned to JTLS and Regions B and C can be taken to JCATS.

➤ *component based sharing of the units and entities:* To simulate everything related to a specific component (e.g. air, maritime, land, psychological operations, special operations etc.) in one of the simulations while simulating the others in another simulation is also an option. For example, we can simulate everything related to special operations component at JCATS, and all the other components at JTLS. In this case, in the same area there may be entities simulated in JCATS and units simulated in JTLS. This increases the probability that an entity in JCATS interact with a unit in JTLS (figure 8).

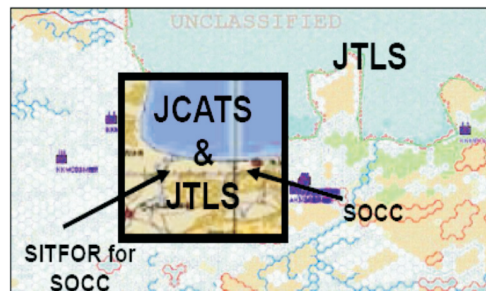


Figure 8: Component based ownership

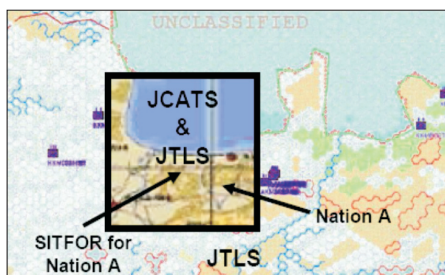


Figure 9: Nation based ownership

➤ *service based sharing of the units and entities:* All the entities for a service can be simulated in a simulation system while all the others are in another simulation system. For example, we can use one of the simulations to simulate maritime operations, and the other for all the other ground and air operations (figure 10).



Figure 10: Service based ownership

➤ *type of operations based on sharing of the units and entities:* Finally operations like counter improvised explosive devices (counter IED), long distance reconnaissance, time sensitive targeting, joint personnel recovery, river crossing, amphibious, riot control can be simulated in JCATS and the others in JTLS (figure 11).



Figure 11: Operations based ownership

Advantages of Multi-resolution Federations

High-resolution constructive simulations are very often called *tactical simulations*. Therefore, it is argued that only highly aggregated simulations are needed for operational and higher-level exercises, and multi-resolution federations are not useful. Although high-resolution simulations fit better for the simulation requirements of tactical level exercises, this perception is not true because of the following two reasons:

➤ In exercises conducted in operational and higher level, MEL/MIL includes many incidents high resolution in nature, such as, *time sensitive targeting (TST)* and *joint personnel recovery (JPR)*. In some operational level exercises, these types of incidents become the majority in MEL/MIL.

➤ In CAX RC interact with simulations, which means that the plans of RC are entered into simulation. This implies that the simulated objects are minimum two levels below the lowest level TA in command hierarchy.

Before further elaborating this, we first would like to list major advantages of multi-resolution federations:

- Better simulation environments, i.e. reasons 1 and 2: It enables simulating also high-resolution incidents more realistically in operational and higher level exercises.
- Enhanced interoperability and reusability: New capabilities can be added into a federation made up of both legacy and state-of-the-art simulation systems. The simulation environment becomes less dependent on a specific simulation.

- Multi-level training environments especially for combined operations: It supports training multiple echelons that have separate sets of training objectives at the same exercise.
- High-resolution results to stimulate high-resolution C2 systems: They can provide both highly aggregated and high-resolution results to stimulate C2 systems.
- Better virtualisation capabilities for operational and higher level exercises: Virtualisation tools like VBS2 can become a federate to these federations.

Tools like VBS2 can provide intelligence products, such as aerial pictures and video streams from *unmanned aerial vehicles (UAV)*. Visualisation of the battlefield can also help the training audience to have a better insight about the possible results of their decisions.

All these are important and worth investing in them. We will focus on the first and the last items in the rest of this section. We will use one example incident that is very common in operational and higher level CAXs: *time sensitive targeting (TST)*. On this example, we will explain what if there is no simulation support, there is only a highly aggregated simulation (JTLS), there is only a high-resolution simulation (JCATS) and there is a multi-resolution federation (NTF).

In our incident (*figure 12*), an intelligence is received by a joint force command (our primary TA): “An important target is in a small village and will presumably stay there several hours”. The TA assesses the situation and possible *courses of actions (COA)*. One of COAs is “to order an air strike”.

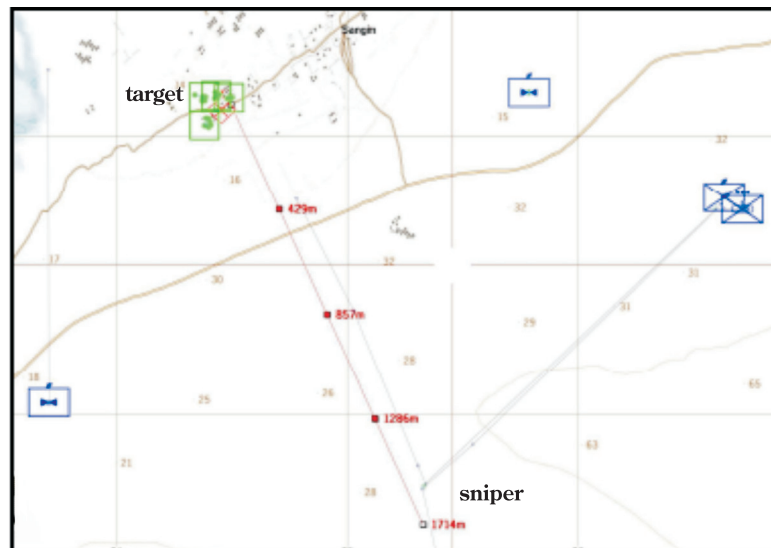


Figure 12: TST incident

Since the risk of collateral casualties is high, this COA is not selected. Another COA is “to order a sniper attack”. This COA seems viable. *Special operations component command (SOCC)*, who is among the primary TA, consults that they can deploy a sniper team to the vicinity of target in time. SOCC is ordered to plan and conduct the operation. SOCC plans the deployment, which also includes deploying helicopters for evacuation and *close air support* in case of an escalated contact and casualties.

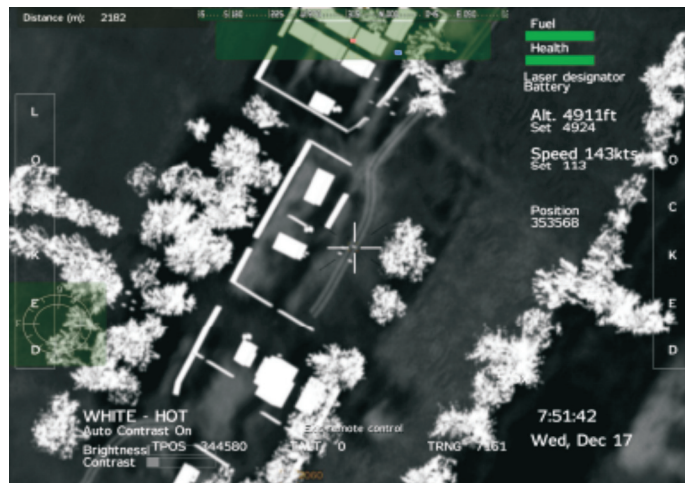


Figure 13: Live simulated video stream from a UAV simulation

SOCC passes the orders to its subordinates who are role players in SOCC RC. SOCC RC plans further and reports that the position in the initial plans does not provide the line of sight. After that point, the sniper team needs to move to a better position, which is almost 2 km away from the position in the initial plan. Some part of this final two km must be covered by crawling. Our four cases for this incident are compared in *table 3*.

Table 3 shows that the best option to simulate a TST incident during an operational level exercise is a multi-resolution federation. When a multi-resolution federation is carefully designed and complemented with effective exercise processes, it can become very cost efficient and useful in support of combined/joint operational and higher level exercises. Please note again that there is not only TST, which response cells in an operational level exercise need to deal with in high resolution. Reader should also always remember that the plans of the training audience are not entered into the simulation directly. They should first be converted to the plans of response cells acting as the subordinates for TA.

Giving examples for the other way around, i.e. why multi-resolution federations are useful in tactical level training is also possible. Expeditionary forces that need

Cases	Comments
No Simulation	<p>SOCC RC and other related RC carries out all the following computation manually and reports back to SOCC, i.e. TA:</p> <ul style="list-style-type: none"> - The availability of aircraft, fuel, ammunition and personnel for the mission including the aircraft for close air support and evacuation. - Line of sight and range assessments. - Threats (sensing, detecting, engaging, probability of hit and kill in case of engagements) and their impacts during the deployments through air. - The time needed for air deployment. - Manual updates of C2 tools for all movement based on the air assets and their link capabilities. - The time needed for the final 2 km. - Threats (sensing, detecting, engaging, probability of hit and kill in case of engagements) and their impacts during the final 2 km. - Positive identification of target. - Collateral casualties. <p>No live video streams from unmanned aerial vehicles (UAV), such as the one shown in <i>figure 13</i>, can be provided.</p>
Highly Aggregated Simulation	<p>SOCC RC carries out all the following manually because highly aggregated simulations do not have the required resolution for modelling these accurately:</p> <ul style="list-style-type: none"> - Line of sight and range assessments. - Threats (sensing, detecting, engaging, probability of hit and kill in case of engagements) and their impacts during the final 2 km. - Positive identification of target. - The collateral casualties.
High-Resolution Simulation	<p>High resolution simulations can model accurately and in the required level of resolution everything listed above. However, the database preparation and operating the model may become too cumbersome because of the overall level of the exercise. Moreover a high resolution constructive simulation system may not have visualisation tools for positive identification and live video streams from UAVs.</p>
Multi-Resolution Federation	<p>This is the right combination. Whenever higher resolution is required the simulation responsibilities are passed to high-resolution simulations. Video streams are provided through a visualisation system like VBS2. Intel products for battle damage assessment (BDA) can also be provided. Moreover, the architecture supports interoperability and reusability.</p>

Table 3: Comparison of types of simulations

long distance transportation, logistics and communications is an example for that type of use cases. Another one can be the use of *low overhead drivers* like JLOD to simulate the civilian traffic and non-kinetic aspects during a tactical training. Since this topic is not within the scope of this paper, we do not elaborate those examples further.

*

Several multi-resolution federations have been developed for the last decade. Most of them are not mature yet, and only few are used in a major exercise. NTF is a multi-resolution federation derived from JMIRM, and used in support of a major NATO exercise in 2008. For the time being, NTF is an HLA federation of JTLS and JCATS. VBS2 is also federated into NTF through DIS. NTF can cover all the required resolution levels in a major combined and joint exercise. NTF is a cost effective simulation tool, and more flexible comparing to any single simulation system or single resolution federation.





THE THINK TANKS AND CIVIL SOCIETIES PROGRAM 2009

European Think Tanks: Regional and Trans-Atlantic Trends (IV)

Greece (35)

Andreas G. Papandreou Foundation (AFP)
Center for Democracy and Reconciliation
in Southeast Europe (CDRSEE)

Center for International and European
Economic Law (CIEEL)

Centre for European Constitutional Law,
Themistocles and Dimitris Tsatsos Foundation
Centre for International Politics Thessaloniki
(CIPT)

Centre for Political Research and Information
Centre of Planning and Economic Research
(KEPE)

Constantinos Karamanlis Institute
for Democracy Defense Analysis Institute (IAA)

Euro-Mediterranean Network for Youth
Trafficking Prevention

E21, Centre for the Development of Ideas
for Greece in the 21st Century

Foundation for Economic & Industrial
Research (IOBE)

Foundation for Mediterranean Cooperation
(FMC)

Greek Centre of European Studies
and Research (EKEME)

Greek Committee for International Détente
and Peace (EEDYE)

Forum for the Modernization of Our Society
(OPEK)

Hellenic Centre for European Studies
(EKEM)

Hellenic Foundation for European
and Foreign Policy (ELIAMEP)

Hellenic Institute of Strategic Studies
(HELISS)

Hellenic Leadership Institute (HLI)

Institute for Balkan Studies (IMXA)

Institute for Strategic and Development
Studies (ISTAME)

Institute of International Economic Relations
(IIER)

Institute of International Relations (IIR)

International Centre for Black Sea Studies
(ICBSS)

Kokkalis Foundation

Lambrakis Foundation (LF)

Liberty Net

National Centre for Social Research (EKKE)

Nicos Poulantzas Institute

Research Center for Gender Equality
(KETHI)

Research Centre for Minority Groups
(KEMO)

Research Institute for American and European
Studies (RIEAS)

Society for Social and Economic Studies
(EKOME)

World Peace Council (WPC)

Hungary (40)

Antall Jozsef Foundation
Batthyany Lajos Foundation (BLF)
Budapest Economics
Center for Educational Policy Analysis (CEPA)
Center for Policy Studies
Center for Strategic and Defense Studies
Centre for Security and Defense Studies
DEMOS Hungary Foundation
Environmental Management and Law Association (EMLA)
Eotvos Karoly Public Policy Institute Financial Research Co.
Foundation for a Civic Hungary (PMA)
Foundation for Market Economy (FME)
Free Europe Centre
Freedom House
Hungarian and Central European International Studies Center
Hungarian Economic Research Co. (GKI)
Hungarian Institute of International Affairs
Institute for Strategic and Defence Studies
Institute for Transitional Democracy and International Security
Institute for World Economics of the Hungarian Academy of Sciences
Institute of Economics of the Hungarian Academy of Sciences
Institute of Political Science of the Hungarian Academy of Sciences
Institute of Sociology, Hungarian Academy of Sciences; Research Group for Sociology of Organisation and Work
International Center for Economic Growth, European Center (ICEG)
Kopint-Datorg Economic Research, Marketing and Computing Company Ltd.
Kopint-Tarki Conjunction Research Co.
Local Government Initiative Development Limited (LGID)
Manfred Wornor Institute
Marmol Research
Metropolitan Research Institute
Miklos Zrinyi National Defence University

Political Capital Policy Research & Consulting Institute
Public Policy Institute
Szabo Miklos Liberal Foundation
Szazadveg Policy Research Center (SZAZADVEG)
Tancsics Mihaly Foundation
TARKI Social Research Centre
Teleki Laszlo Institute
Tocqueville Research Center (T-RC)

Iceland (7)

Andriki
Centre for Social and Economic Research (RSE)
Icelandic Human Rights Centre
Institute of Economic Studies (IoES)
Peace 2000 Institute
Stefansson Arctic Institute (SAI)
University of Akureyri Research Institute (UARI)

Ireland (14)

Centre for Peace and Development Studies
Comhlámh
Dublin European Institute
Economic and Social Research Institute (ESPI)
Edmund Burke Institute
Freedom Institute (LIQUIDATED)
Institute of European Affairs (IEA)
Institute of Public Administration (IPA)
Irish Peace Institute
National Committee for the Study of International Affairs (Royal Irish Academy)
Open Republic Institute
Policy Institute at Trinity College, Dublin
Social Science Research Centre (SSRC)
World Future Studies Federation

Italy (88)

Adam Smith Society
Ambiente Italia Research Institute/Istituto di Ricerche Ambiente Italia
Archivio Disarmo (AD)

- Aspen Institute Italia
Associazione Italiana per la Ricerca Industriale (AIRI)
Assonime (Association for Italy's limited liability companies)/Associazione Italiana fra le Società per Azioni
Center for Constitutional Studies and Democratic Development
Center for Peace Research
Centre for Migration Studies (CSER)/Centro Studi Emigrazione Roma (CSER)
Centre for Research in Law (AREL)/Agenzia di Ricerche e Legislazione (AREL)
Centre for Social Studies and Policies (CENSIS)/Centro Studi Investimenti Sociali (CENSIS)
Centre for Studies in International Politics (CeSPI)/Centro Studi di Politica Internazionale (CeSPI)
Centro Culturale Casa A. Zanussi Pordenone
Centro di Formazione Studi (Formez)
Centro di Ricerca e Documentazione "Luigi Einaudi"
Centro di Studi Aziendali e Amministrativi
Centro Europa Ricerche (CER)
Centro Italiano di Formazione Europea
Centro Regionale di Studi e Ricerche Economico Sociali (CRESA)
Centro Statistica Aziendale
Centro Studi Internazionali
Centro Studi Operazioni Amministrative "Giorgio Constantino"
Centro Studi PIM per la programmazione dell'Area Metropolitana Milanese
Centro Studi Politeia
Centro Studi Unioncamere
CLEs (Centro di Ricerche e Studi sui Problemi del Lavoro, dell'Economia e dello Sviluppo)
Consorzio per gli Studi Universitari in Verona
Demoskoepa/Demoskoepa: Istituto per le ricerche sociali e di mercato
EuroMeSCo
European University Institute (EUI)
Federcasa
Fondazione Aldo Della Rocca
Fondazione Aristide Merloni
Fondazione Eni Enrico Mattei (FEEM)
Fondazione Giangiacomo Feltrinelli
Fondazione Giacomo Brodolini
Fondazione Giovanni Agnelli
Fondazione Giovanni Michelucci
Fondazione Giuseppe Corazzini
Fondazione IARD
Fondazione Ideazione
Fondazione Istituto Antonio Gramsci
Fondazione Istituto Carlo Cattaneo
Fondazione Istituto Piemontese Antonio Gramsci
Fondazione Italianeuropei
Fondazione Liberal
Fondazione Luigi Einaudi
Fondazione Mario e Georgio Labò
Fondazione Regionale Pietro Seveso
Forum on the Problems of Peace and War
Giuseppe Impastato Sicilian Centre of Documentation/Centro Siciliano di Documentazione "Giuseppe Impastato" (CSD)
Il Mulino Institute for Geopolitical and Geoeconomic Studies
Ipalmo Institute for Relations between Italy and the Countries of Africa, Latin America, and the Middle and Far East (IPalmo)
Institute of International Affairs
Institute of Study and Documentation on the European Community and Eastern Europe/Istituto di Studi e Documentazione sull'Europa comunitaria e l'Europa Orientale
International Centre for Economic Research (ICER)
International Institute of Humanitarian Law/Istituto Internazionale di Diritto Umanitario
International School of Disarmament and Research on Conflicts (Isodarco)
Istituto Bruno Leoni
Istituto di Ricerche Economiche e Sociali
Istituto di Ricerche Economiche e Sociali del Friuli Venezia Giulia (IRES-FVG)
Istituto di Studi Giuridici
Istituto di Studi Giuridici Regionali (ISGRE)
Istituto Per Gli Studi Di Politica Internazionale (ISPI)

Istituto per gli Studi sui Servizi Sociali (ISTISSS)

Istituto per la Ricerca Sociale (IRS)

Istituto per lo Studio dei Trasporti nell'Integrazione Economica Europea (ISTIEE)

Istituto Regionale di Ricerca della Lombardia (ICER)

Istituto Siciliano di Studi Politici ed Economici (ISSPE)

Italian Center for Peace Studies

Italian Institute for Cooperative Studies

Luigi Luzzatti/Istituto Italiano di Studi Cooperativi "Luigi Luzzatti"

Italian Peace Research Institute

Italian Society for International Organisation (SIOI)/Società Italiana Per L'Organizzazione Internazionale (SIOI)

Limes

Military Centre for Strategic Studies (CeMiSS)/Centro Militare di Studi Strategici (CeMiSS)

NATO Defense College

Nomisma

OIKOS – International Foundation for Ecological Economics

Pio Manzù Centre/Centro Pio Manzù

Planning Studies Center/Centro di Studi e Piani Economici

Prometeia, Associazione per le Previsioni Econometriche

Robert Schuman Centre for Advanced Studies, European University Institute

Rosselli Foundation/Fondazione Rosselli

Sago, Società di ricerca applicata per il settore della Sanità

South Tyrolean Institute of Ethnic Groups

Third World Academy of Sciences (TWAS)

Kosovo (3)

Kosovar Institute for Policy Research and Development (KIPRED)

Kosovar Research and Documentation Institute (KODI)

Riininvest Institute for Development Research

Latvia (9)

Baltic Center for Strategic Studies

Centre for European and Transition Studies (CETS)

Centre for Public Policy PROVIDUS

Economists Association 2010

Institute Latvia – Public Policy Research Institute

Institute of Economics, Academy of Science (IEAS)

Latvian Centre for Human Rights (LCHR)

Latvian Institute of International Affairs

Media Institute

Liechtenstein (2)

Konjunkturforschungsstelle Liechtenstein (KOFL)

Liechtenstein-Institut

Lithuania (13)

Civil Society Institute CIVITAS

Economic Research Center

Economics Institute

Institute of Defense Technologies

Institute of Democratic Politics (IDP)

Institute of International Relations and Political Science

Institute of Labor and Social Research

Lithuanian Energy Institute (LEI)

Lithuanian Free Market Institute (LFMI)

Lithuanian Regional Research Institute

National Development Institute

New Economy Institute

Public Policy and Management Institute, Velnis (PPMI)

Luxembourg (6)

Centre de Recherche Public de la Santé, CRP-Santé/Public Research Centre for Health

Centre de Recherche Public Henri Tudor (CRP)/Public Research Center Henri Tudor

Institut Pierre Werner

International Network for Studies in Technology, Environment, Alternatives, Development (INSTEAD)/Centre d'Etudes

de Populations, de Pauvreté et de Politiques Socio Economiques (CEPS)

Le Centre de Recherche Public
– Gabriel Lippmann

Luxembourg Institute for European and International Studies/Institut d'Études Européennes et Internationales du Luxembourg

Macedonia, Former Yugoslav Republic of (15)

Analytica
Association for Democratic Initiatives
Association for Modern Economy
Center for Civic Initiative (CCI)
Center for Environmental Law and Public Participation Center for Research and Policy Making (CRPM)

Euro-Balkan Institute
European House Skopje
FORUM – Center for Strategic Research and Documentation

Foundation Open Society Institute (FOSIM)
Institute for Democracy, Solidarity and Civil Society

Institute of Economics
International Center for European Culture Euro-Balkan

Market Economics and Democracy Institute
Ohrid Institute for Economic Strategies and International Affairs

Malta (4)

Diplo Foundation
European Documentation and Research Center, University of Malta
Foundation for International Studies
Mediterranean Academy of Diplomatic Studies

Moldova (5)

Association for Participatory Democracy (ADEPT)

Center for Strategic Studies and Reforms (CISR)

Foundation for Social and Economic Research
– CASE Moldova

Institute for Development and Social Initiatives (IDIS) “Viitorul”

Institute for Public Policy (IPP)

Monaco (0)

Montenegro (4)

Center for Democratic Transition (CDT)
Center for Democracy and Human Rights (CEDEM)

Center for Entrepreneurship and Economic Development (CEED)

Institute for Strategic Studies and Projections (ISSP)

Netherlands (57)

Advisory Council on Science and Innovation Policy (AWT)

African Studies Centre

Alfred Mozer Foundation (AMS)

Centre for Development Planning (CDP)

Centre for European Security Studies

Centrum voor Internationaal Conflict – Analyse & Management (CICAM)

Centre for International Development

Issues Nijmegen

Cicero Foundation

Civilistisch Appèl (Formerly Civilistische Liga)

Cross Cultural Bridges

Development Research Institute (IVO)

Dutch Centre of Political Participation (IPP)/
Instituut voor Publiek en Politiek (IPP)

ECORYS Nederland

Edmund Burke Foundation/Edmund Burke Stichting

Energy Research Centre of the Netherlands (ECN)

Erasmus Center for Financial Research (ECFR)

European Centre for Conflict Prevention

European Centre for Development Policy Management (ECDPM)

European Centre for Work and Society (ECWS)

- European Cultural Foundation (ECF)
European Independent Institute
European Institute of Public Administration (EIPA)
European Research Centre on Migration and Ethnic Relations (ERCOMER)
Evert Vermeer Stichting (EVS)
Frédéric Bastiat Stichting
Germany Institute of the University of Amsterdam (DIA)
Guido de Brès-Stichting, Scientific Bureau of the SGP
Hague Centre for Strategic Studies (HCSS)
Health Council of the Netherlands
Institute of Political Science
Institute of Social Studies
Institutum Europaeum
International Institute for Asian Studies (IIAS)
Mr. G. Groen van Prinsterer Stichting (Wetenschappelijk Instituut van de ChristenUnie)
National Institute for Public Health and the Environment (RIVM)
Netherlands Atlantic Association
Netherlands Bureau for Economic Policy Analysis (CPB)
Netherlands Institute of International Relations "Clingendael"
Netherlands Scientific Council for Government Policy (WRR)
Netherlands Society for Nature and Environment/Stichting Natuur en Milieu
Rathenau Instituut
Research Center for Turkestan and Azerbaijan (SOTA)
Roosevelt Study Center
Royal Netherlands Society for Military Art and Science
Social and Cultural Planning Office of the Netherlands
Social and Economic Council of the Netherlands (SER)
Stichting Libertarisch Centrum Nederland
Stichting Maatschappij en Onderneming (SMO – Society and Enterprise Foundation)
- Stichting Toekomstbeeld der Techniek (STT – Netherlands Study Centre for Technology Trends)
Stichtingen voor Vrijheid en Veiligheid (Foundations for Freedom and Security – OSL)
T. M. C. Asser Instituut
Telders Foundation/Teldersstichting
Tinbergen Institute
Transnational Institute (TNI)
Wetenschappelijk Bureau de SP
Wetenschappelijk Instituut voor het CDA
Wiardi Beckman Foundation
- Norway (15)**
ARENA – Centre for European Studies
CIVITA – Center for Business and Society
Fafu Institute
Fridtjof Nansen Institute (FNI)
Institute for Alternative Development Research (IADR)/Institut for Alternativ Utviklingsforskning
Institute for Social Research (ISF)
International Peace Research Institute, Oslo (PRIO)
Liberalit Forskningsinstitutt (LIFO)
Nordic Institute for Women's Studies and Gender Research (NIKK)
Norut NIBR Finnmark
Norwegian Defence Research Establishment/Forsvarets Forskningsinstitutt (FFI)
Norwegian Institute for Defence Studies (IFS)
Norwegian Institute for Strategic Studies (NORISS)
Norwegian Institute of International Affairs (NUPI)
Norwegian Social Research (NOVA)
- Poland (41)**
Adam Smith Research Centre
Applied Research Center Ultex Ankieter Ltd.
Baltic Institute Center for International Relations

Center for Public Opinion Research
Center for Social and Economic Research
(CASE: Poland)
Centre for Eastern Studies
Centre for Europe – Warsaw University
Centre for European Regional and Local
Studies (EUROREG)
Centre for Political Thought
Cracow Real Estate Institute (CREI)
DEMOSKOP (Market and Social Research)
European Center Natolin
European Institute
Foreign Trade Research Institute
Foundation Globalization Institute
Gdansk Institute for Market Economics
(GIME)
Institute for Private Enterprise and Democracy
(IPED)
Institute for Strategic Studies
Institute for Study on the Foundation
of Democracy
Institute for Sustainable Development
Institute for Western Affairs
Institute of Developing Countries
Institute of Public Affairs
Institute of Regional and Global Studies
International Center for Development
of Democracy
Koszalin Institute of Comparative European
Studies
Lech Walesa Institute
Mareco Polska
Polish Association of Political Science
Polish Council of European Movement
Polish Economic Society
Polish European Community Studies
Association
Polish Institute of International Affairs
Polish Ludwig von Mises Institute
Polish Robert Schuman Foundation
Sobieski Institute
South-Eastern Research Institute
Transformation, Integration and Globalization
Economic Research (TIGER)

Transparency International Polska
World Economy Research Institute (WERI)

Portugal (19)

Causa Liberal
Centre for Research and Studies in Sociology
(CIES)
Centre for Social Studies (CES)
Centre of Research on European
and International Economics (CEDIN)
Centro de Estudos Africanos (African Studies
Centre) (CEA)
Centro de Estudos Africanos (CEA)
Centro de Estudos de Gestao (CEGE)
– Management Research Centre
Centro de Estudos sobre Africa
e do Desenvolvimento (CEsA)
Centro de Investigacao sobre Economia
Portuguesa (CISEP)
Eurodefense Portugal
Euro-Mediterranean Study Commission
Forum de Administradores de Empresas
(FAE)
Institute of European Studies
of the Universidade Católica Portuguesa
(IEE/UCP)/Instituto de Estudos Europeus
da Universidade Católica Portuguesa (IEE/UCP)
Institute of International and Strategic
Studies (IEE)
Institute of Social Sciences, University
of Lisbon (ICS)
National Defense Institute/Instiuto da Defesa
Nacional
Portuguese Institute for International Relations
and Security (IPRIS)
Portuguese Institute of International Relations/
Instituto Português de Relações Internacionais
SOCIUS – Centro de Investigação
em Sociologia Económica e das Organizações

Romania (54)
Association for International Law
and International Relations (ADIRI)
Casa NATO
Catalactica Association

- Center for Defence and Security Strategic Studies
Center for Euro-Atlantic Studies of the University of Bucharest
Center for Institutional Analysis and Development – CADI
Center for Political Studies and Comparative Analysis (CPSCA)
Center for Rural Assistance (CRA)
Center for Social Science Research CENTRAS
Civitas Foundation for Civil Society
Cluj Center for Policy Analysis
Conflict Prevention Center
EURISC Foundation
EUROED Foundation
Eurolink – House of Europe
European Institute of Romania
Euroregional Center for Democracy
Foundation for Democratic Change (FDC)
German Romanian Interdisciplinary Research Institute
Initiative for Democracy in Eastern Europe (IDEE)
Institute for Economic Forecasting
Institute for Marketing and Polls
Institute for Political and Economic Research
Institute for Political Studies of Defence and Military History
Institute for Public Policy
Institute for Quality of Life
Institute for World Economy
Institute of Administration Science “Paul Negulescu”
Institute of Business and Public Administration
Institute of National Economy (INE)
Intercultural Center of Timișoara
International Center for Entrepreneurial Studies
Ludwig van Mises Institut
Manfred Werner Euro-Atlantic Association
Military Higher Education and Research Institute at the “Nicolae Bălcescu” Land Forces Academy
Military Technical Academy
National Administration Association
Pro-Europe League
Public Policy Centre (CENPO)
Research Centre on Interethnic Relations (CCRIT)
Resource Center for Public Participation
Romania Think Tank
Romanian Academic Society
Romanian Center for Economic Policies
Romanian Center for Global Studies
Romanian Foreign Trade Center
Romanian Foundation for Democracy
Romanian Institute for International Studies
Romanian Institute for Recent History
Romanian Institute of Economic and Social Research and Polls
Romanian Society of Political Science
Social Democrat Institute Foundation “Ovidiu Șincai”
Transparency International (TI)
- Russia (109)**
Academy of Political Science
Agency of Social Information
Andrei Sakharov Foundation
Association for Studies in Public Economics
Association of European Studies
Association of the Independent Centers of Economic Analysis
Carnegie Moscow Center
Centre for Analysis of Strategies and Technologies (CAST)
Center for Applied Studies and Policy Improvement (CASPI)
Center for Economic and Financial Research (CEFIR at NES)
Center for Ethnopolitical Regional Studies
Center for European Studies
Center for European Studies
Center for Fiscal Policy
Center for Independent Social Research
Center for Labor Market Studies
Center for Legal Support to Local Government
Center for Macroeconomic Analysis and Short-Term Forecasting

- Center for Political and International Studies
Center for Political Technologies
Center for Regional Economic Studies (CRES)
Center for Social and Economic Expertise
Center for Social and Strategic Studies
Center for Strategic and Global Studies
Center for Strategic Research
Center for the Development of Democracy and Human Rights
Center of Information Technologies
Center of Social Analysis and Reconstruction
Central Economics and Mathematics Institute
Centre for Integration Research and Projects (CIRP)
Centre for International and Regional Policy
Citizens' Watch
Council for Location of Productive Forces
Development Center, Economic Research Foundation
Diplomatic Academy of the Ministry of Foreign Affairs of Russia
Econometric Unit "*Vedi*"
Economic Expert Group
Economic Research and Economic Informatization Center "*Open Economy*" Fund
Economic Research Institute Far Eastern Branch
Eurograd Institute
Expert Institute
Far Eastern Center for Economic Development
Foreign Policy Association
Foundation "*Mother's Right*"
Foundation for Effective Policy
Foundation Politica
Free University
Gorbachev Foundation
Hayek Foundation
INDEM Foundation Center for Applied Political Studies
Independent Actuarial Information-Analytical Center
Independent Institute for Social Policy (IISP)
Institute for Comparative Social Research
Institute for Economic Strategies
Institute for Economic Studies, Kol'sky Scientific Center, RAS
Institute for Economy in Transition
Institute for Financial Studies
Institute for Humanitarian Communication (IHC)
Institute for Humanities and Political Studies
Institute for Industrial and Market Studies
Institute for Private Sector Development and Strategic Analysis
Institute for Problems of Regional Economy
Institute for Stock Market and Management
Institute for the US & Canada Studies
Institute for Urban Economics
Institute of Contemporary Development (INSOR)
Institute of Economic Analysis (IEA)
Institute of Economics & Industrial Engineering
Institute of Europe-Russian Academy of Sciences
Institute of Far Eastern Studies
Institute of International Affairs (IIAP)
Institute of Int'l Economic & Political Studies
Institute of Latin America at the Russian Academy of Sciences
Institute of Law and Public Policy
Institute of Market Problems
Institute of Oriental Studies
Institute of Parliamentary Sociology
Institute of Political Studies
Institute of Science, Innovation and Socio-Economic Programmes
Institute of Socio-Economic and Humanitarian Problems
Institute of Strategic Studies and Analysis
Institute of World Economy and International Relations
Institute of State and Law at the Russian Academy of Sciences
International Center for Human Values
International Centre for Social and Economic Research "*Leontief Center*"
International Foundation for Economic and Social Reforms

- Kaliningrad Chamber of Commerce & Industry
Kaliningrad Regional Economic Development Agency
Levada Center
Moscow Public Science Foundation (MPSF)
Moscow School of Political Studies
National Project Institute "Social Contract"
PIR Center-Center for Policy Studies in Russia
Public Center for Legal and Judicial Reforms
Public Opinion Foundation
ROMIR Monitoring
Russian Chamber of Commerce and Industry
Russian Independent Inst. of Soc. & Natl. Problems
Russian International Studies Association
Russian Political Science Association
Russian Public Opinion Research Center (VCIOM)
Russian Public Policy Center Foundation
Russia's Institute for Strategic Studies
Russo-American Research and Educational Center
St. Petersburg Scientific Center
St. Petersburg Sociological Research Center
St. Petersburg's Centre "Strategy"
Ural Foundation for Social Innovations
- San Marino (0)**
- Serbia (24)**
Argument. Research and Analytical Center
Belgrade Circle
Belgrade Centre for European Integration
Center for Civil-Military Relations (CCMR)
Center for Democracy Foundation
Center for Development of Non-profit Sector
Center for Free Elections and Democracy (CESID)
Center for Liberal-Democratic Studies
Center for Policy Studies
Center for Strategic Studies (CSS)
Economic and Social Policy Institute (ESPI)
Economics Institute
European Movement in Serbia
- Free Market Center
G17 Institute
Humanitarian Law Center (HLC)
Iniciativa Kosovare per Stabilitet (IKS)
Institute for European Studies
Institute for Philosophy and Social Theory
Institute of International Politics and Economics
Management Center
ProConcept
Public Administration and Local Government Center (PALGO)
Transparency Serbia
- Slovakia (18)**
Center for Economic Development (CED)
Centre for Advanced Studies
Centre for European Policy
Civic Association Rural Parliament
Conservative Institute of M.R. Stefanik
F.A. Hayek Foundation – Bratislava
Forum Minority Research Institute (FMRI)
Institute for Economic and Social Reforms (INEKO)
Institute for Liberal Studies/ Young Liberals (Mladí liberáli)
Institute for Public Affairs (IVO)
League of Human Rights Advocates
MESA 10 – Centre for Economic Analyses
Pontis Foundation
Slovak Foreign Policy Association (SEPA)
Slovak Governance Institute
Slovak Institute for International Studies
S.P.A.C.E., n.o. – Social Policy Analysis Centre
Transparency International Slovakia (TIS)
- Slovenia (19)**
Academic and Research Network of Slovenia (ARNES)
Centre for Cultural and Religious Studies (CRS)
Centre for International Cooperation and Development (Center za mednarodno sodelovanje in razvoj)

- Centre for Methodology and Informatics (CMI)
Centre for Strategic Studies
Defence Research Centre
Educational Research Institute (ERI)
Enterprise Institute
Institute Carantania
Institute for Civilization and Culture
Institute for Economic Research/Inštitut za ekonomska raziskovanja
Institute for Ethnic Studies/Inštitut za narodnostna vprasanja (INV)
Institute for European Studies/Inštitut za evropske študije
Institute for Strategic Studies (ISS)
Institute of Social Sciences
International Institute for Middle-East and Balkan Studies (IFIMES)
International Relations Research Centre (IRRC)/Centre of International Relations Peace Institute/Mirovni Institute
Public Opinion and Mass Communication Research Centre (CPOMC)
- Spain (50)**
Anselmo Rubiralta Center for Globalization and Strategy
Asociación de Investigación y Especialización sobre Temas Iberoamericanos (AIETI)
Bancaja International Center for Peace and Development
Center for Analysis of Security
Centre de Recerca en Economia Internacional (CREI)
Centro de Estudios Andaluces
Centro de Investigación para la Paz (CIPFUHEM)
Centro de Investigaciones Sociológicas (CIS)
Centro Internacional de Toledo para la Paz (CIT)
Centro Superior de Estudios de la Defensa Nacional (CESEDEN)
CIDOB Foundation/Fundació CIDOB
Círculo de Empresarios
- Development Assistance Research Associates (DARA)
Elcano Royal Institute of International and Strategic Studies/Real Instituto Elcano de Estudios Internacionales y Estratégicos
Escola de Cultura de Pau (ECP)
Foment del Treball Nacional
Fundació Catalunya Oberta
Fundació Rafael Campalans (FRC)
Fundacion Alternativas
Fundación Humanismo y Democracia
Fundación José Ortega y Gasset
Fundación Pablo Iglesias
Fundación para el Análisis y los Estudios Sociales (FAES)
Fundación para las Relaciones Internacionales y el Diálogo Exterior (FRIDE)
Fundacion Seminario de Investigacion para la Paz (Fundacion SIP)
Galician Institute for International Security and Peace Studies/Instituto Galego de Estudos de Seguranca Internacional e da Paz (IGESIP)
Galician Institute of Analysis and International Documentation/Instituto Galego de Análise e Documentación Internacional (IGADI)
Gernika Gogoratz
Group for Strategic Studies (GEES)/Grupo de Estudios Estratégicos (GEES)
Institución Futuro/Institution Future
Institut Europeu de la Mediterrania (IEMed)
Institut Universitari d'Estudis Europeus
Institute for European Studies/Instituto de Estudios Europeos
Institute for European-Latin American Relations
Instituto Ciencia y Sociedad (INACS)
Instituto Complutense de Estudios Internacionales (ICEI)
Instituto de Cuestiones Internacionales y Política Exterior (INCIPE)
Instituto de Estudios Políticos para América Latina y África (IEPALA)
Instituto de la Paz y los Conflictos
Instituto Español de Estudios Estratégicos (IEEE)

- Instituto Juan March de Estudios e Investigaciones
Instituto Universitario de Economía de Mercado (IUDEM)
Instituto Universitario de Estudios Internacionales y Europeos “Francisco de Vitoria”
Instituto Universitario “General Gutiérrez Mellado”
Juan de Mariana Institute (IJM)/Instituto Juan de Mariana (IJM)
Poder Limitado
Public-Private Sector Research Center (SP-SP)
Real Academia de Ciencias Morales y Políticas (RACMYP)
Research Unit on Security and International Cooperation (UNISCI)
Spanish Centre for International Relations
- Sweden (74)**
Arbetslivsinstitutet
Beijer International Institute of Ecological Economics
Bertil Ohlin-Institute
Captus
Center for Pacific Asia Studies (CPAS)
Center for Public Sector Research (CEFOS)
Center for Research in International Migration and Ethnic Relations (CEIFO)
Centre for Ethics and Economics
Centre for European Labour Market Studies
Centre for Labour Market Policy Research (CAFO)
Centre for Multiethnic Research
Centre for Political Communication Research (CPCR)
Centre for Research on Bilingualism Centre for Community Development and Mobilization (Cesam)
City-VITALity-Sustainability (CITIVAS)
Collegium for Development Studies
Contra Foundation
Dalarna Research Institute (DFR)
Eudoxa
European Institute of Japanese Studies (EIJS)
Forsknings Råds Nämnden (FRN)
Forum Syd
Future Report
Global Water Partnership
Gothenburg School of Economics
Group for Research on Peace and Security Policy
Hagness International AB & Insight Center
Hållbarhetsrådet: Swedish Council for Sustainable Development
Institute for Central Asian and Caucasian Studies
Institute for Futures Studies
Institute for International Economic Studies (IIES)
Institute for Labour Market Policy Evaluation (IFAU)
Institute for Management of Innovation and Technology
Institute of Economic Research
International Institute for Democracy and Electoral Assistance (IDEA)
International Organisation for Knowledge Economy and Enterprise Development (IKED)
Jarl Hjalmarsson Stiftelsen
Kvinna till Kvinna
Life & Peace Institute (LPI)
MENA.SE (Middle East and North Africa)
Mistra
Sektor 3
FOI Swedish Defence Research Agency
National Institute of Economic Research
New Welfare/Den Nya Välfärden
Nordic Africa Institute
Olof Palme International Center
Peace and Conflict Research Institute (Department of Peace and Conflict Research)
Peace and Development Research (PADRIGU)
Peace Research Institute
Raoul Wallenberg Institute of Human Rights and Humanitarian Law
Ratio
Research Institute of Industrial Economics
Research Policy Institute

International Connections

- Royal Swedish Academy of Agriculture and Forestry
SISU Idrottsutbildarna
Stockholm Centre for Organizational Research
Stockholm Environment Institute (SEI)
Stockholm Institute of Transition Economics (SITE)
Stockholm International Peace Research Institute (SIPRI)
Stockholm International Water Institute (SIWI)
Stockholm School of Economics (Department of Economics and Health Economics)
Studieförbundet Näringsliv och Samhälle (SNS)
Swedish Co-operative Institute (KOOPI)
Swedish Foundation for Small Business Research
Swedish Institute for European Policy Studies (SIEPS)
Swedish Institute for Growth Policy Studies (ITPS)
Swedish Institute for Social Research (SOFI)
Swedish Institute of International Affairs
Swedish Network for European Studies in Economics and Business
Swedish Peace and Arbitration Society (SPAS)
Timbro
Transnational Foundation for Peace and Future Research (TFF)
Weapons of Mass Destruction Commission
- Switzerland (71)**
Asia Research Centre
Avenir Suisse
Center for Asian Studies (formerly Modern Asia Research Center)
Center for Comparative and International Studies
Center for Security Studies and Conflict Research (Center for Security Studies)
Centre de Recherches Entreprises et Sociétés (CRES)
- Centre for Applied Studies in International Negotiations (CASIN)
Centre for Development and Environment (CDE)
Centre for Economic and Ecological Studies (Cen2eco)
Centre for Energy Policy and Economics (CEPE)
Centre for Humanitarian Dialogue
Centre for Migration Research (CSERPE)
Center for Our Common Future (CFOCF)
Club of Rome
Comprehensive Dialogue among Civilizations
The Crisis and Risk Network (CRN) (the former Comprehensive Risk Analysis and Management Network)
Eranos Foundation
Europe-Third World Centre (Centre Europe-Tiers Monde (CETIM))
Evian Group at IMD
Geneva Centre for Democratic Control of Armed Forces (DCAF)
Geneva Centre for Security Policy
Geneva International Academic Network (RUIG-GIAN)
Geneva International Centre for Humanitarian Demining
Geneva International Peace Research Institute
Global Forum for Health Research
Global Public Policy Institute
Gottlieb Duttweiler Institut (GDI)
Graduate Institute of International and Development Studies/Institut de Hautes Etudes Internationales et du Développement
Imagination Lab Foundation
Institut Constant de Rebecque
Institut de Recherches Économiques (IRENE)
Institut d'Économie et Management de la Santé (IEMS)
Institut d'Études Politiques et Internationales
Institute for Economy and the Environment
Institute for Islamic and Middle Eastern Studies
Institute for Media, Peace & Security
Institute of Political Science

- Institute of Federalism
Interdisziplinäre Grundlagenforschung
über Ursachen gewaltsamer Konflikte
International Centre for Monetary and Banking
Studies (ICMB)
International Centre for Trade and Sustainable
Development (ICTSD)
International Relations and Security Network
(ISN)
International Risk Governance Council
Liberales Institut
Military Academy (MILAK)
Modern Asia Research Center (MARC)
NORRAG – Network for Policy Research,
Review and Advice on Education and Training
Oikos – International Student
Organization for Sustainable Economics
and Management
Ostasiatisches Seminar der Universität Zürich
Paul Scherrer Institut
Pro Libertate
Prognos
Programme for Strategic and International
Security Studies (PSIS)
RAFAD Foundation
Recherches en Economie et Management
de l'Environnement (REME)
Schweizerisches Institut für Auslandsforschung
(SIAF)
Small Arms Survey
St. Gallen Centre for Futures Research (SGZZ)
Swiss Academy for Development
Swiss Agency for Development
and Cooperation (SDC)
Swiss Foreign and Security Policy Network
(SPN)
Swiss Forum for International Affairs (FSPI)
Swiss Forum for Migration and Population
Studies (SFM)
Swiss Institute for Business Cycle Research
(KOF)
Swiss Institute for International Economics
and Applied Economic Research
Swiss Peace Foundation/Schweizerische
Friedensstiftung
- Swiss Research Institute of Small Business
and Entrepreneurship (KMUHSG)
Swiss Tropical Institute (STI)
Thurgauer Wirtschaftsinstitut
Wintherthur Institute of Health Economics
World Trade Institute
- Ukraine (45)**
Agency for Legislative Initiatives
Agency of Humanitarian Technologies
Consulting Group
Agency of the Regional Development “Donbas”
All-Ukrainian Charitable Fund “*Ukrainian
Legal Foundation*”
Bukovina Partnership Agency
Center for Anticrisis Studies
Center for Comparative Social Research
– CESSI
Center for Economic Development
Center for International Security and Strategic
Studies (CISSS)
Center for National Security Studies
Center for Peace, Conversion and Foreign
Policy of Ukraine
Center for Political and Legal Reforms (CPLR)
Center for Political Studies
Center for Political Studies (Lviv)
Center for Social and Economic Research
(CASE-Ukraine)
Center for Social Studies (“*Sofiya*”)
Center for the Study of Regional Policy
Crimean Center for Independent Research
Democratic Initiatives Foundation
Dnipropetrovsk Center of Social Research
East Ukrainian Foundation for Social Research
Europa XXI Foundation
Geneza – Social and Humanities Consortium
Institute for Economic Research and Policy
Consulting
Institute for Euro-Atlantic Cooperation
Institute for Reforms
Institute for Regional and Euro-Integration
Studies “*EuroRegio Ukraine*”
Institute of Election Law
Institute of Global Strategies

- Institute of Politics
International Centre for Policy Studies
International Institute of Comparative Analysis
International Research and Training Center
for Information Technologies and Systems
Kiev Center of Political Studies
and Conflictology
Kiev Economics Institute
Kiev International Institute of Sociology
Market Reforms Center
National Institute for Strategic Studies (NISS)
Penta Political Consulting Bureau
Politological Innovation Centre
SOCIS – Center for Social and Political
Investigations
Ukrainian Centre for Economic and Political
Studies named after Olexander Razumkov
Ukrainian Center for Independent Political
Research (UCIPR)
Ukrainian Centre for International Security
Studies
Ukrainian Centre of Political Management
- United Kingdom (285)**
Aberystwyth Department of International
Politics
Acronym Institute for Disarmament Diplomacy
Adam Smith Institute
Anglo-German Foundation for the Study
of Industrial Society (AGF)
Arab Research Centre
Arab World Documentation Unit (formerly
Centre for Arab Gulf Studies)
Bertrand Russell Peace Foundation
Bevan Foundation
Biodiversity and Economics for Conservation
(BIOECON)
Bosnian Institute
Bow Group
British Institute of Human Rights (BIHR)
British Institute of International
and Comparative Law (BIICL)
British-American Security Information
Council
Brooks World Poverty Institute (BWPI)
- Bruges Group
Callaghan Centre for the Study of Conflict
Catalyst
Centre for Arab and Iranian Studies
Centre for Asia Pacific Studies (CAPS)
Centre for Associative Economics
Centre for Civil Society
Centre for Conflict and Peace (formerly
Centre for Conflict Analysis)
Centre for Conflict Resolution
Centre for Contemporary European Studies
Centre for Defence and International Security
Studies
Centre for Defence Economics
Centre for Defence Studies
Centre for Democracy and Development
(CDD)
Centre for Democratization Studies
Centre for Development Policy and Research
(CDPR)
Centre for Development Studies
Centre for Ecology Law & Policy
Centre for Economic Performance (CEP)
Centre for Economic & Social Inclusion
Centre for Economic Policy
Centre for Economic Policy Research
Centre for Economic Reform and Transition
(CERT)
Centre for Energy Policy and Technology
Centre for Euro-Asian Studies
Centre for European and Comparative
Governance
Centre for European Reform
Centre for Federal Studies (CFS)
Centre for Global Energy Studies (CGES)
Centre for Global Political Economy (CGPE)
Centre for Health and International Relations
(CHAIR)
Centre for Health Economics
Centre for Health Services Research (CHSR)
Centre for History and Economics
Centre for Independent Transport Research
(CILT)

- Centre for Intelligence and International Security Studies
- Centre for International Development
- Centre for International Studies
- Centre for Lebanese Studies
- Centre for Local Economic Strategies
- Centre for Peace & Reconciliation Studies
- Centre for Performance Evaluation and Resource Management (CPERM)
- Centre for Policy Evaluation (CPE)
- Centre for Policy Modelling
- Centre for Policy on Ageing
- Centre for Policy Studies
- Centre for Public Policy and Management (CPPR)
- Centre for Regional, Economic and Social Research (CRESR)
- Centre for Research into Post-Communist Economies (CRCE)
- Centre for Research and Analysis of Migration (CReAM)
- Centre for Research in Economic Development and International Trade (CREDIT)
- Centre for Research in Ethnic Relations (CRER)
- Centre for Research into Economics and Finance in Southern Africa
- Centre for Research on Inequality, Human Security and Ethnicity (Queen Elizabeth House)
- Centre for Rural Research (CRR)
- Centre for Scottish Public Policy (CSPP)
- Centre for Security Studies
- Centre for Social and Economic Research on the Global Environment (CSERGE)
- Centre for Social Justice
- Centre for Socio-Legal Studies
- Centre for Studies in Democratization
- Centre for Studies in Security and Diplomacy
- Centre for Sustainable Urban and Regional Futures (SURF)
- Centre for Swiss Politics
- Centre for the Study of African Economies
- Centre for Study of Economic and Social Change in Europe (CSESCE)
- Centre for the Study of European Politics, Security and Integration
- Centre for the Study of Financial Innovation
- Centre for the Study of Global Governance
- Centre for the Study of Globalisation and Regionalisation
- Centre for the Study of Public Policy (CSPP)
- Centre for the Study of Radicalisation and Contemporary Political Violence
- Centre for the Study of Regulated Industries (CRI)
- Centre for the Study of Terrorism and Political Violence
- Centre for Urban and Regional Studies (CURS)
- Centre on Skills, Knowledge and Organisational Performance (SKOPE)
- CentreForum
- Chatham House (Royal Institute for International Affairs)
- Chronic Poverty Research Centre (CPRC)
- CIVITAS
- Civitas International – Researchers Without Borders
- Commonwealth Policy Studies Unit (CPSU)
- Community Development Foundation
- Conflict Studies Research Centre
- Conservative Policy Forum
- Constitution Unit
- Corner House
- Council for Arab-British Understanding (CAABU)
- Council on Christian Approaches to Defence and Disarmament
- Counterpoint
- Crime and Society Foundation (CSF)
- Crisis States Research Centre
- Cunliffe Centre
- David Davies Memorial Institute
- David Hume Institute
- Democratic Audit
- Democratic Dialogue
- Demos

Department of Criminology (formerly the Scarman Centre)	Hansard Society
Department of International Development/Queen Elizabeth, Oxford University	Harvard Sussex Program on Chemical and Biological Weapons
Department of Peace Studies	Health and Social Care
Development Research Centre on Migration, Globalisation & Poverty	Health Economics Research Group (HERG)
Development Studies Institute	Health Economics Research Unit (HERU)
E.G. West Centre	Henry Jackson Society
Earthwatch Institute (Europe)	HLSP Institute
Economic and Social Research Council	Human Rights Centre
Economic Organisation and Public Policy Programme (EOPP)	Humanitarian Practice Network
Economic Research Council	Information Assurance Advisory Council (IAAC)
Economic Research Institute of Northern Ireland (ERINI)	Institute for African Alternatives (IFAA)
Ekklesia	Institute for Conflict Research
ESRC Centre for Competition Policy	Institute for Development Policy and Management (IDPM)
European Council on Refugees and Exiles	Warwick Institute for Employment Research
European Development Policy Study Group	Institute for Employment Studies
European Development Research Network	Institute for European Environmental Policy
European Foundation	Institute for Fiscal Studies
European Institute	Institute for German Studies
European Policy Forum	Institute for International Policy Analysis (IFIPA)
European Studies Centre	Institute for Jewish Policy Research
Fabian Society	Institute for Policy and Practice (IPP)
Federal Trust for Education and Research	Institute for Political & Economic Governance
FIELD	Institute for Public Policy Research
First Defence	Institute for Social Inventions/Global Ideas Bank
Foreign Policy Centre (FPC)	Institute for War and Peace Reporting
Forum for the Future	Institute of Arab and Islamic Studies
Foundation for Law, Justice & Society	Institute of Commonwealth Studies
Fraser of Allander Institute	Institute of Development Studies
Glasgow Centre for the Child & Society	Institute of Economic Affairs
Global Britain	Institute of Employment Rights
Global Business Research Institute	Institute of Ideas
Global Policy Institute	Institute of Irish Studies
Globalisation Institute	Institute of Muslim Minority Affairs
Gold Mercury International	Institute of Welsh Affairs
Governance and Social Development Resource Centre (GSDRC)	International African Institute
Green Alliance	International Alert
Green Economics Institute	International Boundaries Research Unit
Gulf Centre for Strategic Studies	International Centre for Corporate Social Responsibility
	International Centre for Security Analysis

International Conflict Research (Incore)	Oxford Institute for Energy Studies
International Futures Forum	Oxford Research Group
International Institute for Environment & Development (IIED)	OXONIA – Oxford Institute for Economic Policy
International Institute for Strategic Studies	Panos Institute
International Migration Institute (IMI)	Pensions Institute
International Policy Network	Personal Social Services Research Unit (PSSRU)
International Security Information Service (ISIS)	Police Foundation
Joseph Rowntree Foundation	Policy Exchange
Jubilee Centre	Policy Institute
Jubilee Research	Policy Network
King's Fund	Policy Research Bureau CLOSED IN MARCH 2007
Labour Research Department	Policy Research in Engineering, Science and Technology (PREST)
Leverhulme Centre for Research on Globalisation and Economic Policy (GEP)	Policy Research Institute
Liberal Bangla	Policy Studies Institute
Libertarian Alliance	Politeia
Localis	Post-war Reconstruction and Development Unit
London Middle East Institute, SOAS University of London	Public Services International Research Unit Reform
London School of Economics Hayek Society	Refugee Studies Centre
Low Pay Commission	Regulatory Policy Institute (RPI)
LSE Hellenic Observatory	Relationships Foundation
LSE Public Policy Group	Richardson Institute: Research in Peace Studies and Conflict Resolution
Margaret Thatcher Foundation	Royal Commission on Environmental Pollution
Migration Research Unit	Royal United Services Institute for Defence and Security Studies
Minority Rights Group International	Runnymede Trust
Mountbatten Centre for International Studies Mutuo	Saferworld
National Centre for Social Research (NatCen)	Science and Technology Policy Research (SPRU)
National Institute of Economic and Social Research	Scientific Alliance
New Economics Foundation	Scientists for Global Responsibility (SGR)
New Health Network	Scottish Council Foundation
New Local Government Network	Scottish Economic Policy Network
New Policy Institute	Smith Institute
New Politics Network	Social Affairs Unit
Nexus	Social Issues Research Centre
Nordic Policy Studies Centre	Social Market Foundation
Open Europe	Social Policy Research Unit (SPRU)
Optimum Population Trust	Sovereignty
Overseas Development Group (ODG)	
Overseas Development Institute (ODI)	
Oxford Council on Good Governance	

Stockholm Network	Wellbeing in Developing Countries ESRC
Strategic and Combat Studies Institute (SCSI)	Research Group
Study of Parliament Group	Wellcome Trust
Sussex Centre for Migration Research	Welsh Centre for International Affairs (WCIA)
Tavistock Institute	Westminster Foundation for Democracy
Transport 2000	Wilton Park
UK Centre for Evidence Based Policy and Practice (Evidence Network)	Young Foundation
VENEZIE Institute	Vatican City (1)
Verification Research, Training and Information Centre (VERTIC)	Caritas Internationalis
	TOTAL THINK TANKS: 1,750

Acknowledgements

I sought and received input from every corner and capital in Europe as I researched and wrote this paper so I am indebted to many people and I just want to acknowledge their help and support. First and foremost, I want to express my deep appreciation to all the scholars, think tank directors, policymakers and donors throughout Europe who took time out of their busy schedules to complete and return our surveys, allowed me to conduct far reaching interviews and provided me with invaluable feedback on this paper. I also want to thank my research interns for their help in collecting and analyzing the data collected for this research project.

Think Tank and Civil Societies Program

“Helping to bridge the gap between knowledge and policy”

The Think Tanks and Civil Societies Program (TTCSP) at the International Relations Program, University of Pennsylvania conducts research on the role policy institutes play in governments and in civil societies around the world. Often referred to as the ‘think tank’s think tank’, TTCSP examines the evolving role and character of public policy research organizations. Over the last 20 years the Think Tanks and Civil Societies Program has laid the foundation for a global initiative that will help bridge the gap between knowledge and policy in critical policy areas such as international peace and security, globalization and governance, international economics, environment, information and society, poverty alleviation and health. This international collaborative effort is designed to establish regional and international

networks of policy institutes and communities that will improve policymaking and strengthen democratic institutions and civil societies around the world. The Think Tanks and Civil Societies Program works with some of the leading scholars and practitioners from think tanks and universities in a variety of collaborative efforts and programs. If you would like additional information about our publications and programs contact Jmcgann@sas.upenn.edu

Research on Think Tanks and Civil Societies

The TTCSP conducts research on the role of think tanks in the policymaking process and as key civil society in countries around the world.

Think Tank Capacity Building Program

The TTCBC conducts research and provides technical assistance on a wide range environmental challenges and organizational development issues facing think tanks and policy communities around the globe. In addition, TTCBC develops and implements strategies that will increase the capacity of think tanks so that they can better serve policymakers and the public.

Database and Directories

The Center developed the first interactive, global, comprehensive, multi-sectoral database and directory of think tanks. Most databases and directory are organized by discipline, country or region. The Center maintains the only multi-sectoral database of think tanks consisting of over 6,000 think tanks in 169 countries. Specialized databases of think tanks in areas such as development, democracy, security, international affairs and health have been created.

ABOUT THE AUTHOR

James G. McGann, Ph.D. is the Assistant Director of the International Relations Program and Director of the Think Tanks and Civil Societies Program at the University of Pennsylvania. He is also a Senior Fellow at the Foreign Policy Research Institute in Philadelphia. For the last 20 years, he has served as President of McGann Associates, a program and management consulting firm specializing in the challenges facing think tanks, policymakers, international organizations and philanthropic institutions.

Dr. McGann has served as a consultant and advisor to the World Bank, United Nations, United States Agency for International Development, Soros, Hewlett

and Gates Foundations and foreign governments on the role of nongovernmental, public policy and public engagement organizations in civil society. He has served as the Senior Vice-President for the Executive Council on Foreign Diplomats, the public policy program officer for The Pew Charitable Trusts, the Assistant Director of the Institute of Politics, John F. Kennedy School of Government, at Harvard University, and a Senior Advisor to the Citizens Network for Foreign Affairs and the Society for International Development.

Among Dr. McGann's publications are *Competition for Dollars, Scholars and Influence In The Public Policy Research Industry* (University Press of America 1995), *The International Survey of Think Tanks* (FPRI, 1999), *Think Tanks and Civil Societies: Catalyst for Ideas and Action*, co-edited with Kent B. Weaver (Transaction Publishers 2000), *Comparative Think Tanks, Politics and Public Policy* (Edward Elgar 2005) http://www.e-elgar.co.uk/Bookentry_Main.lasso?id=2756, *Think Tanks and Policy Advice in the US: Academics, Advisors and Advocates* (Routledge, 2007), *Think Tanks: Catalysts for Democratization and Market Reform* (Forthcoming Routledge 2009), *Global Trends and Transitions: 2007 Survey of Think Tanks* (FRPI 2008), *The 2007 Global Go To Think Tanks* (FPRI 2008), *Think Tank Index* (Foreign Policy Magazine 2009), and *The 2008 Global Go Think Tanks* (2009 IRP University of Pennsylvania), *BRICS and Think Tanks Partners In Economic Development* (CIPE, Summer 2009), *Democratization and Market Reform in Developing and Transitional Countries: Think Tanks as Catalysts* (Routledge Summer 2009) <http://www.routledgepolitics.com/books/Democratization-and-Market-Reform-in-Developing-and-Transitional-Countries-isbn9780415547383>, *Global Think Tanks* (Forthcoming Routledge 2010), *Think Tanks and Policy Advice in the US: Academics, Advisors and Advocates*, <http://www.routledgepolitics.com/books/Think-Tanks-and-Policy-Advice-in-the-US-isbn9780415772280>

RESEARCH INTERNS

Helen Ayres (University College London)
Jonathan de Jong (University of Pennsylvania)
Jared Miller (University of Pennsylvania)
Jonathan Owen (Villanova University)
Emily Phillips (Bryn Mawr University)
Alba Topallaj (University of Pennsylvania)
Krzysztof Walski (University of Pennsylvania)

THINK TANKS AND CIVIL SOCIETIES PROGRAM © 2009, TTCSP

All rights reserved. Except for short quotes, no part of this document and presentation may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, recording, or by information storage or retrieval system, without written permission from the Think Tanks and Civil Societies Program.

**All requests, questions and comments should be
emailed to:**

James G. McGann, Ph.D.

Director

Think Tanks and Civil Societies Program 2009

International Relations Program

University of Pennsylvania

Telephone: (215) 746-2928 / (215) 898-0540

Email: Jmcgann@sas.upenn.edu



MILESTONES IN THE HISTORY OF THE ROMANIAN NAVAL FORCES

Commander Dr Olimpiu Manuel GLODARENCO
Dr Florin STAN

The authors of this article wish to point out the significance of the Romanian Naval Forces within the national defence system. First, they write about the tasks of the Romanian Navy during the War of Independence. Then, they mention the Romanian Navy missions during the First World War and the War of National Unification. Moreover, they take an approach to the Interwar Naval Doctrine, emphasising the Romanian navy modernisation programmes during 1918-1941 and the naval actions during the Second World War. In the end of the article, they reflect on the evolution of the Navy from the post-war period to nowadays, drawing attention to the outstanding contribution of our country to BLACKSEAFOR

Keywords: *naval doctrine; military flotilla; naval procurement programme; naval aircraft; coast defence*

In agreement with its own general interest, each country adopts a military doctrine that represents that country's conception of its national defence system. Within this doctrine, for maritime countries, a naval doctrinal component stands distinctively¹. Setting up the Romanian united flotilla during Alexandru Ioan Cuza² and gaining the state independence in 1877-1878 – which also brought back Dobrogea within the country's boundaries – created favourable prerequisites for the development of the Romanian Navy.

Although until the period between the two World Wars we did not have a clear Romanian naval doctrine, we could say that the statement of the great political personality Mihail Kogălniceanu – *“The key to our salvation is the seaway”* – largely defined the importance and significance of the Romanian maritime interest during those years.

Commander Dr Olimpiu Manuel Glodarenco – Director, the Romanian Navy Museum, University Reader at “Andrei Șaguna” University, Constanța.

Dr Florin Stan – Head of the History Section, the Romanian Navy Museum.

¹ Contraamiral Prof. dr. Gheorghe Marin (coord.), *Marea Neagră, spațiu de confluență a intereselor geostrategice*, Editura Centrului Tehnic Editorial al Armatei, București, 2005, p. 247.

² ***, *Monitorul Oastei*, I (1860), no. 41 on 22 October, p. 698; Georgeta Borandă, *Colonelul Constantin Petrescu, primul comandant al flotei muntenesti și comandant al flotei Principatelor Unite*, in *Anuarul Muzeului Marinei Române*, tome V, 2002, pp. 235-238.

After the very first acquisitions³ that shaped the nucleus of an active military flotilla⁴, the years when Romania got involved in the new Balkan crisis, which was reopened between the Ottoman Empire and the Russian Tsarist Empire, allowing our state to become independent, proved that the Romanian state needed a consistent naval force able to protect its national boundaries.

The Romanian Military Flotilla's missions and actions during the War of Independence showed that a naval doctrine had to effectively sustain the general efforts of the nation towards the defence of its fundamental interests.

Missions and Actions of the Romanian Navy during the War of Independence

During the War of Independence (1877-1878), the actions of the Romanian naval forces consisted both in risky missions for the strategic protection of the Danube line and in actual fighting actions, especially during the operations from Plevna and Vidin, when they directly contributed to the enemy's defeat⁵. On the night of 13 to 14 May 1877, a remarkable group of mosquito-craft led by "RÂNDUNICA" attacked by surprise and finally sank the enemy Turkish armour-plated gunboat "HIVZI RAHMAN"⁶. This success eased the action of the Romanian ships, which, during the strategic protection operations of the Danube, installed mine barrages in different locations on the river, transported troops, war techniques and ammunition, materials used to build the boat bridges across the river.

After the second Ottoman monitor, "PODGORIȚA", one of the most powerful firing ships on the Danube, was sunk by the mortar battery "PERSEVERENȚA" on 7 November 1877, the Romanian Navy limited the Turks' manoeuvre and action possibilities on the river⁷.

The War of Independence showed that a strong Danube fleet was needed, and the re-inclusion of Dobrogea within the national boundaries opened significant

³ Căpitan-comandor dr. Marian Moșneagu, *Evoluția Marinei Militare Române în perioada 1860-1914*, in *Anuarul Muzeului Marinei Române*, tome III/1, 2000, pp. 135-136.

⁴ ***, *Statul Major al Forțelor Navale. 1860-2005. Tradiții și perspective*, Editura Centrului Tehnic-Editorial al Armatei, București, 2005.

⁵ Cristian Crăciunoiu, Raymond Stănescu, *Oțel, aburi și torpile. Marina română în războiul de independență. 1877-1878*, Editura Modelism, București, 2001.

⁶ Georgeta Borandă, *Contribuții la istoricul confruntărilor navale de pe Dunăre, din anul 1877 – partea I*, in *Anuarul Muzeului Marinei Române*, tome IV, 2001, pp. 94-95.

⁷ *Ibid*, part II, in *Anuarul Muzeului Marinei Române*, tome V, 2002, pp. 103-104.

development perspectives to the Navy, including the need to organise a sea fleet. This imposed the adoption of corresponding procurement programmes, 3 of such plans being adopted between 1878 and 1916⁸.

War Flotilla Modernisation Programmes during 1878-1916

Between the War of Independence (1877-1878) and the War of Unification, three naval procurement programmes were accomplished within the Military Flotilla⁹. The first programme was adopted in 1880 and aimed at providing the Maritime Flotilla with ships necessary for its specific activity. At that moment, the brig “*MIRCEA*” remarkably entered service (in 1882), standing for a traditional symbol school-ship for the training of the Romanian Navy staff.

As new credits for the growth of the fighting ships fleet were granted, the year of 1887 represented the beginning of the second flotilla procurement programme. We should underline that the battle-cruiser “*ELISABETA*” entered service in 1888¹⁰.

The third Navy procurement programme started in 1906¹¹, when a financial funding was obtained with the purpose of constructing new ships. This way, in 1907, 4 monitors (“*AL. LAHOVARI*”, “*I. C. BRĂTIANU*”, “*L. CATARGIU*” and “*M. KOGĂLNICEANU*”) and 8 safety vedette boats were purchased¹².

Before the first world conflagration, the need to have own naval doctrinal policies was affirmed in texts such as the one named *Misiunea Marinei noastre – The Mission of our Navy* (1909), which underlined that *the most secure way to progress is the joint parallel development of Navy and industry*. The controversial matter

⁸ *Ibid*, p. 117.

⁹ Căpitan-comandor (r.) dr. Ion Ionescu, *Primele elemente și principii ale doctrinei navale românești (1878-1916)*, in *Anuarul Muzeului Marinei Române*, tome VIII, 2005, p. 153.

¹⁰ Prof. dr. Valentin Ciorbea, *Crucișătorul “ELISABETA” – de la idee la construcție*, in *Anuarul Muzeului Marinei Române*, tom IV, 2001, pp. 165-170. Expatriated upon in Valentin Ciorbea, Georgeta Borandă, *Istoricul crucișătorului “ELISABETA”*, Ovidius University Press, Constanța, 2004.

¹¹ The year 1906, the fortieth year of the kingdom of Carol I, marked the beginning of the second flowering epoch of the Romanian Navy, its existence being then funded on the real grounds of its call to protect the national sea and river shores. His Majesty noticed with content the progress made by the Romanian Navy and, through his speech at the launching of the *SMRROMANIA* ship in Constanța, he expressed his will that the commercial marine should grow in peacetime, under the full shield and protection of the Navy.

¹² Specialist in Museography Cornel Greavu, *Programele navale în marina română. 1880-1943*, in *Anuarul Muzeului Marinei Române*, tome II, 1999, pp. 151-158. The vedette boats equipping the Navy in 1907 were named after heroes of the War of Independence, fought in 1877-1878: Maj. Ene Constantin (V1), Capt. Nicolae Lascăr Bogdan (V2), Capt. Mihail Romano (V3), Maj. Dimitrie Giurescu (V4), Maj. Gheorghe Șonțu (V5), Maj. Nicolae Grigore Ioan (V6), Lieut. Dimitrie Călinescu (V7) and Capt. Valter Mărăcineanu (V8).

regarding the size of the maritime fleet was considered in relation with the political needs of the country, sustaining, however, that *“only when we raise our Navy to an appreciated rank and the Danube’s mouths are sufficiently protected and when this protection stretches and ties to the fortification flank will we have the right to feel proud to be the Danube’s sentinel”*.

The missions accomplished by the Romanian Navy units during the War of Unification confirmed this conclusion.

The Romanian Navy during the War of National Unification

During the First World War, the Romanian Navy accomplished a wide range of missions, the most important being the following: the attack against the Austro-Hungarian fleet at Rusciuk on 14 August 1916, the action of the Danube Escadrille’s ships, which defended the bridgehead from Turtucaia and safeguarded the Romanian troops’ withdrawal out of this area, the supporting action of the right wing of the land army located in Dobrogea by the ships of the Operation Navy under the fire of the German artillery¹³.

Referring to the way in which the fleet supported our land troops, being able to resist under the fire of seven heavy German batteries, in his memoirs, Rear-Admiral N. Negrescu¹⁴ showed that: *“The days when the left wing of the German army was chased and the days of Rasova will write everlasting glory pages for our small, but brave and tireless Romanian flotilla”*.

Even though during the autumn of 1916 the fleet had had certain success, being able to advance under the fire of German batteries and even to free a number of Dobrogea localities previously conquered by enemies, it ceased its offensive actions in December 1916, while the Romanian army withdrew to Moldova for recovery and limited its actions to defensive operations, based especially upon the evacuation of the entire ship fleet of the Navy on the Chilia branch.

In 1917, the Navy, together with the Army, contributed to defending the Danube front, bombing with its ships’ artillery the enemy’s batteries located in Tulcea, as well to securing the water transportation between Galați and the Danube’s mouths.

During the last year of war (1918), the fleet was given the most difficult mission, namely to clear the mines off the Danube and the sea, to restore navigation ways in peacetime.

¹³ Căpitan-comandor Ion Ionescu, *Concluziile reieșite din participarea marinei române la Primul Război Mondial*, in *Anuarul Muzeului Marinei Române*, tome III/2, 2000, p. 187.

¹⁴ About the commanders of the Navy units during the First World War, Căpitan-comandor (r.) Nicolae C. Petrescu, *Cu tricolorul la catarg. Comandanți ai Marinei Militare în Războiul pentru Întregirea României*, Editura Europroduct, Pitești, 2002.

The Interwar Naval Doctrine

After the national unity was achieved in 1918, the Romanian state had to set its objectives to defend its boundaries by its armed forces.

In the work entitled *Avem nevoie de Marina Militară ? (Do We Need the Navy ?)*, published by Commander E. Roșca and Lieutenant-Commander G. Koslinsky in 1923, the stringent necessity for the creation of a significant Navy was underlined: “*The naval power does not owe either to hazard or improvisation, but results from the scrupulous preparation of its constituent elements. Let us create, then, the Navy we need. Let us set our naval programme, let us form our staff and let us prepare a naval base. Let us prepare the naval power with our entire precaution and perseverance*”¹⁵.

The Romanian naval doctrine imprinted the role the Navy had to play, under the circumstances in which the initial general tendency expressed even from the political scene was to abandon the maritime policy on the grounds that Romania would never have a fleet to confront the most powerful Black Sea riparian state. For the Romanian Navy, the new situation imposed by the enlarged state boundaries reflected in a more complex approach to logistics, which had to be reconfigured, as well as in the modernisation and renewal measures of its techniques and procurement means.

After 1918, the security and protection of the new boundaries of Greater Romania had as political, military and economic support the system of peace treaties adopted within the *Paris Peace Conference (1919-1920)*, Romania’s accession to the *League of Nations (1919)*, the *defensive Romanian-Polish military conventions* together with the conventions founding the *Little Entente (1921)*. On 25 July 1921, another important act took place: signing the *Paris Convention*, which established the definitive status of the Danube, through which the river navigation was declared free and opened to all flags. The rights were guaranteed by the *Danube European Commission*, headquartered in Galați, for the maritime part of the river, and by *The International Danube Commission* for the “*fluvial Danube*”. We should also mention the conclusion of the *Lausanne International Convention* in 1923 on the Bosphorus and Dardanelles Straits, which stipulated the freedom to navigate for all states’ ships.

In the equation of the new naval doctrine, an outstanding part was the landscape of the Romanian coasts, which were generally open, without any gulfs, islands or other natural harbours that could have offered large

¹⁵ Viceamiral (r.) Constantin Iordache, *Pagini din gândirea navală românească interbelică*, selection, Editura Ex Ponto, Constanța, 2003, p. 28 and the following.

possibilities for harbouring or masking and, for this reason, the defence of the military bases involved an approach to certain defensive measures of the most varied nature. Besides a well-organised system for the protection of coastal ways by the coast artillery, the creation of an efficient surveillance device by patrol ships was also necessary. The possibility to rapidly install mine barrages that would prevent enemies – who aimed to control the interest areas – from coming near the seashore should have been also taken into account. It was equally necessary to create an offensive-defensive system, with ship units (mosquito crafts, submarines and destroyers) that could develop rapid striking possibilities to an as large distance from the Romanian coasts as possible.

From a doctrinal point of view, the manoeuvre applied to the Navy branches had to be reconceived. The coast artillery would have been used under more adequate conditions by equipping it with high calibre cannons and supporting it with land artillery mobile units.

Even though the theory upon *the inferior fleet in action* was not explicitly affirmed¹⁶, the perspective of the vision on the coordination of a Romanian military fleet actions – with the declared purpose to reach competitiveness to defend the integrity of Greater Romania – had the features of such a concept.

As regards defending the border in the Danube area, the Romanian river forces seemed to be insufficient for such a mission, although a part of the intervention area could be excluded thanks to the existing political-military alliance with Yugoslavia. If a war with the Soviet Union had occurred, the foreseen tactical principle would have been to use the river flotilla for the army flank on the river and also to increase the flotilla resistance with complementary fighting means against a more powerful enemy, through mine barrages and coast batteries. If a war with Bulgaria had begun, a less offensive attitude could have been permitted due to a weaker enemy, but only within the borders.

To accomplish these visions, corresponding procurement measures were obviously imposed. The doctrinal requirement relating to performance was materialised through the orders aimed to modernise the heavy artillery equipment in 1937, placed to the Metallurgical Plants in Reșița. The anti-aircraft warfare assets were going to be purchased from Germany and Switzerland.

To defensively protect the seashore, doctrinal orientations required modern compatibilities regarding the Navy fighting forces, but the first option was to use mine barrages – considered efficient and cost-effective warfare assets, available

¹⁶ Căpitan-comandor (r.) Ion Ionescu, *Politica navală a României între anii 1919 și 1941*, Editura Companiei Naționale Administrația Porturilor Maritime Constanța SA, Constanța, 2002, pp. 51-52.

to any state with a less developed economy that intended to protect its coastal areas or to forbid navigation in certain districts.

The defence – by artillery, of own mine barrages – and the strikes of the enemy ships approaching the seashore led to the necessity for a new force to be built to face these challenges. This way, as a direct requirement of the naval doctrine, coast artillery units were established and, in 1936, a battery composed of three cannon pieces – 152 mm Armstrong type cannons – was installed in the North of Constanta (“Tataia” area).

The Romanian naval doctrine also required a naval aircraft, as the Navy did not have such a branch, but it had only cooperated with the Hydroaviation Flotilla of the Military Aeronautics, which had as main mission the surveillance of the seashore.

In a conference held in 1928, entitled *The Maritime Power as a Civilisation and National Defence Factor*¹⁷, Commander Ioan Bălănescu, future Commander-in-chief of the Navy during 1934-1938, showed that the maritime power and all the elements that determined the functions of a fleet within the national defence system should arise from the state naval policy. “*The naval policy – the officer affirmed – sets the attitude and development of the maritime power towards the problems of national defence*”. He also showed that: “*We cannot conceive a Merchant Navy without a Navy that has the mission to protect commercial ships and harbours. To defend the Merchant Navy, the Navy should be able to rule the sea and maritime communication means and to use them for its own purposes while forbidding the enemies to do so*”. According to I. Bălănescu, the missions of the Romanian Navy had to be the following: – *securing the maritime communication means for its own traffic; protecting maritime ways in front of the enemy; – defending the seashore or defending the coasts*. To accomplish such missions imposed by the national defence system, our fleet had to be equipped with: *surface boats* (battle cruisers, destroyers, anti-submarine crafts, mine sweeping vessels and mine planters) and *aircraft units* (scout hydroplanes, torpedo-planes and fighting planes). As a conclusion, Commander I. Bălănescu underlined the duty of each Romanian towards the country maritime power regarding the construction of *our Sea Fleet*, its modernisation, the development of the merchant fleet, of harbours ... everything to *spread and uplift the national flag of our Navy on the world seas*¹⁸.

¹⁷ Viceamiral (r.) Constantin Iordache, *op. cit.*, p. 79 and the following.

¹⁸ Maria Petru, *Marina Națională Română – “Lux sau necesitate” (opinii exprimate în perioada interbelică)*, in *Anuarul Muzeului Marinei Române*, III/2, 2000, p. 191.

In 1932, Colonel G. Vizanti and Major Scarlat Urlăţianu, well-known military theoreticians, published the paper *The Romanian Strategy for the Future War* (The Royal Court Publishing House, Bucharest) with a distinct chapter on a Romanian military doctrine. The establishment of an army with naval, land and air forces was considered to be able to precisely meet well-defined political purposes. To shape a military doctrine, it was primarily necessary to set the general framework of the state policy that would have been nothing but the logical conclusion of its international political situation, its national tendencies and aspirations as well as of its internal political situation¹⁹.

In 1936, the evolution of the Romanian-Soviet relations determined the Navy specialists to draft a complex document entitled *Studiu asupra apărării coastelor* (*Study on Coast Defence*) that was a conceptual version related to the maritime-fluvial defensive in case of an open military conflict with the great neighbouring state. This study emphasised some new ideas: transferring forces, making efficient the sea-terrestrial cooperation, increasing the importance of defence bases, delaying the enemy effects in case of landing²⁰.

The beginning of the second world conflagration in 1939 brought again to discussion the maritime-fluvial defence dimension. From a conceptual point of view, during the ardent period between September 1939 and June 1941 (Romania's neutrality and expectation), the existence, composition and strength of the War Navy had to rely on the recognised economic and military interests. The Navy had to fulfil multiple objectives but with a limited number of resources. The satisfactory settlement of such a requirement imposed:

- to know the Romanian maritime and fluvial interests, as well as the interests of possible enemies in the Black Sea area;
- to identify objectives by prioritisation;
- to cover the deficiencies²¹.

Under the given circumstances, the main maritime interests of the country were:

- to benefit from the relation with Bosphorus in order to increase the economic and financial potential;
- to intercept the maritime communications linking the harbours from Caucasus, Crimea, Ukraine to allow the exchange of the military values within this area to the benefit of Romania;
- to defend the seashore against external actions with the purpose of strengthening the land forces and secure their freedom to act on other fighting lines²².

¹⁹ Căpitan-comandor (r.) Ion Ionescu, *op. cit.*, p. 48.

²⁰ *Ibid.*, p. 49.

²¹ *Ibid.*, pp. 57-58.

²² *Ibid.*, p. 58.

The first obstacle was stated to be the adversary forces in relation with both the defence of own interests and the attack of the enemy's interests. The doctrinal conception was completed by the fact that the maritime strategy, unlike the land strategy, allowed the co-existence of two elements: *forces* and *interests*. For this reason, the maritime objectives could be multiple and sometimes contradictory, and setting their importance and order varied depending on the very circumstances. All these ideas and conceptions were exposed in December 1940 within a complex document entitled *Planul de înzestrare al marinei militare (The Navy's Procurement Plan). Hypothesis 15*²³.

Former Minister of War during the Goga-Cuza Government (1937-1938), in 1940, General Ion Antonescu sent a document to the whole army entitled *Directive pentru noua orientare doctrinară a armatei (Guidelines for the New Army Doctrinal Orientation)*, in which the doctrinal requirements were characterised by the increase in that the *offensive* and *cohesive* factors corresponding to the new political orientation the country was heading to at that time. The guidelines explained that the naval doctrine, like the military doctrine, was dictated by the people's needs related to their living and unity, being rather required by possibilities than by intentions²⁴.

In conclusion, we can state that the naval doctrine was a complementary framework to the national military doctrine stating the land forces freedom of action. As the *Guidelines* sent over by General I. Antonescu showed, this was a doctrine of possibilities rather than a doctrine of intentions, which took into account the need of compatibility between its exigencies and application measures into the maritime-fluvial area and the Romanian state's offer to meet all its interests – as there were no objective limits in the economic and financial area.

The most important effect of the naval doctrine was that, during the period preceding the participation of Romania in the Second World War and during the following period, the Navy remained the only element that could have reaffirmed the state sovereignty in the Danube Delta and could have secured the sea and river shores if the land forces in use had been demobilised.

Romanian Navy Modernisation Programmes during 1918-1941

The fourth Navy procurement programme, drafted before the First World War²⁵, which regarded the entering into service of 4 torpedo-boat destroyers to strengthen the maritime defence capacity was not accomplished anymore because of the beginning

²³ *Romanian Military Archives (AMR)*, fund 3837, file no. 2847, f. 16.

²⁴ ****, *Directive pentru noua orientare doctrinară a armatei*, București, 1940, p. 3 and the following.

²⁵ *Romanian Military Archives (AMR)*, fund 2988, file no. 460, f. 60.

of the world conflagration. This programme was partially accomplished only after the war, in 1920, by equipping the Navy with the destroyers “MĂRĂȘEȘTI” and “MĂRĂȘTI”.

In 1924, the fifth naval programme was drafted²⁶, with a several years execution, which regarded, among others, the procurement of 12 submarines, 12 mosquito-crafts, one plane-carrier, but, because of economic and financial reasons, this programme could be only partially developed by purchasing the destroyers “REGELE FERDINAND” and “REGINA MARIA” in 1930, as well as the submarine “DELFINUL” in 1936.

Setting up the Ministry of Air and Navy in 1936 resulted in a deeper concern for the naval development, the sixth naval programme being thus drafted²⁷; this sixth naval programme pursued the construction of certain ships in the country and, in 1928, *The National Fund of the Navy* was set up to efficiently support new ship and harbour arrangement works. Following these measures, in 1939, the minelayer ship “AMIRAL I. MURGESCU” was launched at the Shipyard Galați, and the following year the construction of the submarines “RECHINUL” and “MARSUINUL” started (they became operational in 1943). This support made it possible, at that moment, for Romania to enter the second world conflagration, most of the ammunition necessary to the Romanian artillery being produced in the country, at Reșița where *Wickers* mines (British license, with anchor and contact explosion) were produced for the sea barrages.

The Navy during the Second World War

During the years of the Second World War, the Romanian Royal Navy prevented the Soviet Fleet from controlling the vital area located in the Western and Northwestern basin of the sea. The main missions of our Navy were:

- to stop the attempts to land on the Dobrogea seashore;
- to secure the Danube mouths against possible enemy incursions;
- to secure the maritime transportation to supply the Southern front and the oil ships heading to Bosphorus²⁸.

The Navy actions in the Black Sea during the Second World War – the Eastern campaign – took place during several chronological stages starting from the main

²⁶ *Romanian Military Archives (A.M.R.)*, fund Minister’s office, file no. 506, f. 472.

²⁷ George Petre, Ion Bitoleanu, *Tradiții navale românești*, Editura Militară, București, 1991, p. 228; Specialist in Museography Cornel Greavu, *op. cit.*, p. 157.

²⁸ Căpitan-comandor Dorin Mara, *Marina Regală a României în cel de-al II-lea Război Mondial*, Editura Economică, București, 2000, p. 51 and the following. See also Nicolae C. Petrescu, *Marina română în războiul antisovietic*, Editura Europroduct, Pitești, 2008. We should remember that between 22 June 1941 and 1 September 1943, the activity of the Navy Forces was materialised in 21 586 marching hours while 22 678 sea miles were covered. Transports of 1 773 695 tons (out of which 316 537 tons were carried by Romanian ships) were convoyed. 507 missions were carried, causing enemy losses of 15 submarines, 17 planes, 6 war ships and one commercial ship.

accomplished missions: *22 June – 8 August 1941* was a period during which the navy forces had as main mission the defence of the seashore by counter-attacking the landing attempts on the Romanian seashore; *8 August 1941 – 28 July 1942* was the stage during which the Romanian naval forces mainly secured transports; *28 July 1942 – 5 April 1944* – direct and indirect support missions of the land forces and supplying transports were carried out; *5 April – 13 May 1944* – the sea naval forces took part in the evacuation of the Romanian and German troops from Odessa and Sevastopol; *13 May – 23 August 1944* – seashore defence missions.

One of the events the Romanian Navy took part in during this conflagration was “*Operation 60 000*”, the greatest naval operation in the Black Sea, accomplished between April and May 1944, when the naval forces successfully participated in the evacuation of the Romanian and German troops from Odessa and Sevastopol²⁹. Another outstanding action was the convoying by Sea Division ships – on the seaways – of the ships that carried Jewish emigrants, in 1944. This operation places the Romanian Royal Navy on the front pages of the Second World War annals³⁰.

For the way the Navy acted and accomplished its missions during the years of the Second World War, the Head of State cited, through a *Nation and Army Order of the Day*, the Romanian Royal Navy with *all its naval, air and land units on land and sea for bravery, fighting spirit, competence, initiative, moral and professional qualities*³¹. This Order of the Day no. 54, issued on 10 February 1944, is worth being mentioned *in extenso*: “*The Romanian Royal Navy is cited through a Nation and Army Order of the Day with all its naval, air and land units on land and sea for:*

- *the bravery it demonstrated in fights since the very beginning of the war against an enemy who was superior in number and redoubtable in the war tactics applied;*
- *the fighting spirit and competence held together with its initiative, its higher moral and professional qualities throughout its missions compensating for the quantitative inferiority.*

Due to these qualities, the Royal Navy succeeded in:

- *providing the country and army with seashore inviolability and seaways for war transports that strengthened the action force of all our fighting elements located outside our country;*
- *preventing the enemy from using the seaways for its own purposes.*

*Such sacrifices will stand for the future as an endless source of tradition, which will be the foundation of a new sea destiny of the Romanian people*³².

²⁹ Căpitan-comandor (r.) prof. dr. Jipa Rotaru, căpitan-comandor dr. Ioan Damaschin, *Glorie și dramă. Marina regală română. 1940-1945*, Editura “Ion Cristoiu”, București, 2000, pp. 132-158.

³⁰ Florin Stan, *Portul Constanța – poartă deschisă evreilor spre “fara promisă”. Studii privind “problema evreiască” în România. 1938-1944*, Editura Muzeului Marinei Române, Constanța, 2007, p. 70.

³¹ Căpitan-comandor (r.) prof. dr. Jipa Rotaru, căpitan-comandor dr. Ioan Damaschin, *op. cit.*, p. 243.

³² *Ibid.*

The Navy Evolution during the Post-War Period

On the solid foundation of the lessons learned by the Romanian Navy during the Second World War, several theories were developed after the war about Romania being involved in a possible conflict, a maximum naval procurement programme being then drafted for the Navy, to be accomplished within 10 years. The issue regarding the organisation and efficient use of the Navy forces in a future armed confrontation was aimed at the following operational objectives:

- *maintaining own communication between national harbours;*
- *maintaining external communication through the Bosphorus;*
- *intercepting enemy communications;*
- *defending coasts against possible enemy offensive actions;*
- *attacking enemy coasts and harbours, alone and in cooperation with the land army*³³.

In 1947, the general mission of the Navy was to cooperate in order to defend the sea and river shores during the border security mission, which was assigned to our army forces according to the *Paris Peace Treaty (1947)*. Within the *local border defence action*, the Navy was to stand as a main and conclusive element for the sea front due to its possibilities to extend the sea force action up to the normal limit of the sea border, which was the enemy seashore. In the *Instructions on Fluvial Flotillas* and the *Instructions on Joint Actions of Land Troops and Navy Forces*, drafted in 1953, the *Danube Flotilla* was stipulated to be composed of *ships, air force, land troops and seashore defence units*. According to the *Land Forces Campaign Rules*, the missions of the Navy were:

- *to destroy the enemy ships or installations;*
- *to disorganise the sea enemy communications;*
- *to destroy the enemy military and industrial objectives located on the seashore;*
- *to fight against the enemy air force;*
- *to support the land troops by sea;*
- *to defend the sea installations;*
- *to protect their own sea communications.*

The principles that formed the foundation of crew training tactics followed the Soviet model – as it is well-known, Romania was under the Soviet Union influence. This fidelity, except certain doctrinal tones and operational detachment, survived until the events of December 1989 that brought about the end of the totalitarian socialist regime in Romania.

³³ Expatiated upon in the paper signed by dr. Marian Moşneagu, *Politica navală postbelică a României (1944-1958)*, Editura Mica Valahie, Bucureşti, 2005.

The Revolution of December 1989 put the Navy in action under real fighting conditions. Although 22 December brought about the total commitment of the Armed Forces to the Revolution, since the very beginning of the new democratic regime, starting the very same day, the Romanian Armed Forces were subject to an information war aimed at undermining its actions by providing false information. As to the Navy Command, it took all the measures necessary to make possible a complete victory of the Romanian Revolution. The war ships were alarmed and the seamen secured the most important strategic objectives within their military competence. Special order was given to use war ammunition only in case of extreme necessity.

During the post-December 1989 evolution of the country, the Navy distinguished itself in the Romanian general effort to strengthen its regional stability role, to develop cooperation and dialogue between all the Black Sea states, contributing both to regional security and to good neighbourhood relations; the Black Sea Naval Cooperation Task Group – *BLACKSEAFOR* – the Romanian Navy participated in with specific actions is an outstanding proof in this respect.

Within the context of the military institution reform, the Navy forces became, and not at all accidentally, the first completely professionalised armed forces service.

Since Romania joined the *North Atlantic Treaty Organisation (NATO)*, in 2004, the Romanian Navy tradition and historical values have been capitalised on, together with its NATO allies and Western partners, in the people's interest within the context of globalisation.

The Romanian Navy Forces are currently carrying on the significant tradition of this military service, which aims to meet people's interest and defend generous ideals such as border security, fluvial and maritime security and complex military and diplomatic relations development at the Black Sea and everywhere else Romania places its geostrategic interests.

Selective Bibliography

- ***; Statul Major al Forțelor Navale, *Marea Neagră – spațiu de confluență a intereselor strategice*, Editura CTEA, București, 2005.
- Viceamiral Traian Atanasiu (coordonator), contraamiral dr. Anatolie Zemba, comandor dr. Cornel Mihai, comandor (r.) prof. univ. dr. Vasile Grad, comandor conf. univ. dr. Gheorghe Marin, *Puterea maritimă și diplomația navală*, Editura Militară, București, 1998.
- Viceamiral (r.) Constantin Iordache, *Elemente de strategie maritimă*, Editura Ex Ponto, Constanța, 2000.
- Căpitan-comandor dr. Marian Moșneagu, *Principii doctrinare privind organizarea și misiunile Forțelor Maritime Militare ale României în perioada postbelică (1944-1958)*, in *Buletinul Forțelor Navale*, s. n., no. 7/2007.
- Dr. Vasile Nazare, *Geopolitică și realism politic la Marea Neagră*, in *Anuarul Muzeului Marinei Române*, tome VIII, 2005.

MILITARY JOURNALISTIC UNIVERSE

Armada International, Switzerland, vol. 34,
no. 4, August-September 2010
Command ... Dynamically • What Will They Be Up
to Next? • Nasty and Fired from Under • Corvettes
Can Play Jaws • South Africa's Defence Industry:
Turning the Corner? • Combat Aircraft Fighting
for ... Sales! • The Soldier as Nucleus • Wheels
and Deals at DSA 2010 • Live Field Testing with
Thales • Compendium: Urban Warfare

Homage to General
Marcel Bigeard • Haiti:
French Engineer Troops
Help Rebuilding Schools
• Armed Forces Assist
Flood Victims in Var
Department • Geopolitics
of Caucasus – Interview
• A “Sole Office”
for the Combatant •
Media and Armed Forces
in Afghanistan • Supreme

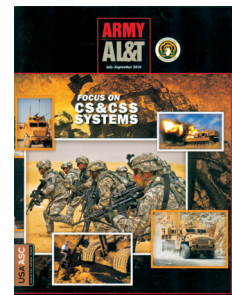
Allied Command – Transformation – Interview
• Formation of Hearing Handicap Persons
for Emergency • Defence Bases – Special Guide •
Tchad: Mirage 2000 Aircraft Replace Mirage F1 •
Strategic Research Institute for Military School
– Technical File • Near Protection for French
Fishing Ships in Indian Ocean • Towards a New
French-African Military Cooperation (File)

Army AL&T, USA, July-September 2010
Program Executive Office Ground Combat Systems
– Our Mission is Our Warfighters' Future • Program

Executive Office Ground
Combat Systems Leads
Combat Vehicle
Modernization • Stryker
Modernization Systems
Development
and Systems Engineering
Requirements Versus
Reality • Forward Repair
Activity-Iraq Drawdown
• Equipping Joint

Warfighters through Modernization of Unmanned
Ground Systems • Commonality of Towed Artillery
Digital Fire Control Systems • Fleet Management
of Tactical Wheeled Vehicles • Fire Suppression
Systems Enhance Tactical Wheeled Vehicles
Survivability • Joint Light Tactical Vehicle
Technology Development Phase Vehicles Delivered
on Schedule, Competitive Prototyping Proves
Fruitful • The Next Generation Automatic Test
Station Offers Organic Off-System Test Capability
for the US Army • Army Rapidly Develops
Expeditionary Fire Suppression Refill Station
• Mine Resistant Ambush Protected Program
Meets Urgent, Changing Requirements • Route
Clearance Vehicles – Fulfilling Simultaneous
Mission WHILE Detecting and Neutralizing
Mines

Ejercito, Spain, no. 832, July-August, 2010
The Multidiscipline in Operations (Integrated
Operations) • The Hybrid Conflict under Review •
Completely Defeating Counterinsurgency



A Courageous Decision on Kosovo • Many Open Questions about the New Structure of the Bundeswehr • How Does Russia See NATO ? Part 2 • Contributions of the Joint Support Service in Operations of the Bundeswehr • Future Gearing of Unmanned Aviation



Systems • *“We Europeans Have the Best Know-how in the Construction of Helicopters”* • EUROFIGHTER in Ongoing Missions and Operations • Command Post System of the Army • EU Battle Groups • Armament Projects of the Army • First Experiences Gained from the Introduction of SASPF in the Joint Support Service • *“MEADS Can be a Core Element of NATO’s Air Defence Capability”* • Risk Communication • The Winner is the Organised Crime • The Islamic Nuclear Power of Pakistan

History of Globalisations: Globalisation – A Political Reading • Monetary Innovations since the Year 1000 to the First World War • China and Globalisation: Crisis Precipitates Mutation of World Economic System • Crisis and Globalisation: Place of Emergent “Second World” and of “Third World” • Crisis, Analyser of World Economy and its Theories • Tragicomedy of Euro • Crisis and Recession in Euro Zone: Another Policy is Possible • Re-creating French Franc to Face the Inevitable News • Afghanistan: the Hard Ransom of “Wise Inertias” • Museums: Mercantile Drift



International Security, USA, vol. 35, no. 1, Summer 2010

Balancing on Land and at Sea: Do States Ally against the Leading Global Power ? • Pyongyang’s Survival Strategy: Tools of Authoritarian Control in North Korea • The Center Still Holds: Liberal Internationalism Survives • The Illusion of Liberal Internationalism’s Revival • Perpetuating US

Pre-eminence: The 1990 Deals to «Bribe the Soviets Out» and Move NATO In • Getting What You Want: Positive Inducements in International Relations

Polish Helicopters to Take MASE Self-Protection Pods to Afghanistan • Thin Blue Line: Israel Navy Looks to Evolve Its Coastal Patrol Capability • Every Dog Has Its Day: Military Working Dogs Bolster Protection in Afghanistan • Oto Melara Unveils



Draco Weapon System for Air Defence on the Move • Battle of the Bulge: Getting to Grips with the Burdens of War • From Design to Life: Start Gun Fires for Type 26 Combat Ship • Keeping an Eye on the World: Pilots Conduct HMD Balancing Act • Shoot for the “Hip”: Resurgent Mi-8/17 Builds on Long Service

Military Review, USA, vol. 90, no. 4, July-August 2010

Security Force Assistance Operations: Defining the Advise and Assist Brigade • Counterinsurgency and Beyond: Operationalizing the Civilian Surge • Let’s Take the French Experience in Algeria Out of US Counterinsurgency Doctrine • Unit of Action: Organizing the Brigade Combat Team for Future Wars • No Simple Solution: Regional Force Operations in Hau Ngia, Vietnam • 2003 Iraq, 1945 Germany, and 1940 France: Success and Failure in Military Occupations • Unmanned Aerial Systems: Quality as well as Quantity • A Primer on Developing Measures of Effectiveness • Persistent Security, Then Development • Human Terrain Team Operations in East Baghdad • Warfare by Internet: The Logic of Strategic Deterrence, Defense, and Attack

Military Technology, Germany, vol. 34, no. 8, 2010

Ballistic Missile Defence Review • Ship-Based BMD • Medium Altitude/Range Air Defence System • MEADS Edges Toward Critical Milestone • The Maturity of OCCAR • The State of Integrated Air and Missile Defence and the Phased Adaptive Approach • Convergence and Battle Command: More Power to the Cutting Edge • Missile Sensor and Homing Systems • Space-Based Persistent ISR

• Israeli's Surveillance Satellites • China's Growing Capabilities • Towards an Exclusive Indian SIGNIT Satellite • RUAG Land Systems: A Swiss Success Story • Soldier Technology 2010 Show Report

Revue Défense Nationale, France, no. 729,
April 2010

Strategic Uncertainties and Political Ambiguities • Political Europe, with the Cards on the Table • *Defence and Partnership*: Public-Private Partnerships: What Role in Reform? • New Engagement Rules and Privatisation: Until Where To Go? • Institutionalised Public-Private Partnerships • *Strategic Neighbourhood*: Eastern Borders of Europe • Caspian Sea, Energetic Axis • Russian Military Doctrine: An Useless Doctrine? • Collective Security Treaty Organisation • *Landmarks, Opinions, Debates*: Considerations on Russia • Security in Europe and Conventional Arms Control • Outsourcing the War? • Risky Society and War • For a Pedagogy of War Violence • Defence and Protection of Biodiversity

Revue Défense Nationale, France, no. 730,
May 2010

French Strategic Competitiveness in the 21st Century • Food Insecurity Could Destabilise the World • Euro-Atlantic Security: A Security for All • *Crisis Management*: Progressive Generalisation of Engagement Rules in NATO • Engagement Rules: A Legal Subject? • About Strategic Influence of Elementary Particles • Engagement Rules: Irregular Rules • *Middle East*: Middle East in a Plight • Iran: What Nuclear Sanctuary? • Yemen: A New Strategic Stake? • The Situation of Mediterranean Strategic Integration • *Landmarks, Opinions, Debates*: The Stakes of a French Military Base in the Persian Gulf • What Reform for the Lebanese Army • A Strategy against al-Qaeda • The Three Levers of Action, according to Marshal Gallieni • Intelligence and Peacekeeping Operations? • Crisis Centre at Quai d'Orsay • *"France-Russia 2010"*: Cooperation and Defence • Art of War in Youngsters under Fifteen

Revue Défense Nationale, France, no. 731,
June 2010

National Basis of Strategic Research • From Satory Plateau to Eurosatory World Armament Exhibition • For the Nuclear Bomb • *Cyber-war*: Can We Dissuade in Cyber Space? • Cyber-war and Cyber

Defence in NATO and EU • Cyber-war and Space War, Future Conflict Bases? • *African Developments*: African Peace and Security Architecture • Security Reform in Guinea • Security and Defence: EU-Africa Relations • *Landmarks, Opinions, Debates*: An European Military Officers' School? • Engagement Rules and Tactics: Honour Serving Complexity • French General Manoeuvre Skills in Counter-insurgency • To Reinforce our Disposition in Afghanistan? • Tactical Drone: Element of Military Power • Pakistan against Terrorism: Perceptions and Realities • War, Crisis and Barbarity • Limits of Anti-terrorism • Resilience: From Concept to Reality • Serbia: Between Integration and Interaction • ESCO under Kazakhstan Presidency • American Nuclear Posture and *Bunkers* Challenge • Again on Iraqi Nuclear Weapons • *Net Assessment* – Prospecting Method used by Pentagon • Copenhagen Syndrome (European Diplomatic Failure)

Myanmar or Burma: Dialogue rather than Sanctions • The *"Tactical"* Legal Advisor in Land Military Operations Abroad • Today's Marshal Cadets • The United States Sergeants Major Academy • Robotics More and More in our Future • EOD

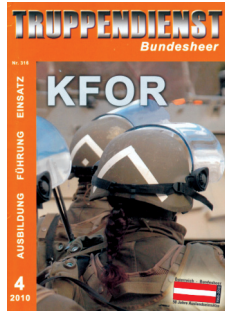


(Explosive Ordnance Disposal) – Special Afghanistan Operation Salam • EOD Special – Operation Salam 2 • EOD Special – The Fight against the Improvised Explosive Devices: Counter-IED • EOD Special – The *"Military Search"* • EOD Special – The New National Centre of Excellence for C-IED • EOD Special – Present and Future of the Engineers – Interview with Brigadier General Antonio Dibello, Inspector of the Engineer Corps • War in Philosophical Thought • Somalia 1995: Operation *"IBIS 3"*

Signal, USA, vol. 64, no. 12, August 2010
Security Comes Standard • The Exception Becomes the Rule • Government Prepares for Work Force Changes • Approval Granted for Private Software to Run in Secure Cloud • Information Dominance Bows to Network

Limitations • Securing America's Defense Computers Becomes Big Business • Army Plans Swat Teams of Mechanical Bugs • A Sensor in Every Pocket • Infrared Sensor Designers Go to the Well • One for the Money, Two for the

The European Armament Industry From World Market Leader to Lagging Competitor • Military Protection of Cultural Property and Military Preservation of Cultural Heritage • Lieutenant General Guido Novak of Arienty • School of Signals • CONRAD – The VHF Radio System of the Austrian Armed



Forces • Information and Communication Technology Security and Information Security in the Austrian Armed Forces • Psychology of Operation – The NATO Working Group • The Austrian Armed Forces in Kosovo • Assignment with the CJPOTF in Afghanistan • Hanging by a Thread

World Policy Journal, USA, vol. 27, no. 2,
Summer 2010

The Big Question: How To Solve the Health Crises • Anatomy of a Pandemic: Tuberculosis • Healing People: India on \$30; Brazil on \$300; France on \$3 000 • Lethal Counterfeits • Ghana: The Waste Land • Palestine: From the Rubble, Life • The Last Yakuza • Abkhazia on Three Wheels • The Forever War: Inside India's Maoist Conflict • So Europe Ends at the Bosphorus ?

Selection and Translation

Delia PETRACHE,

Dr Mihai POPESCU, Cătălina ROJIȘTEANU

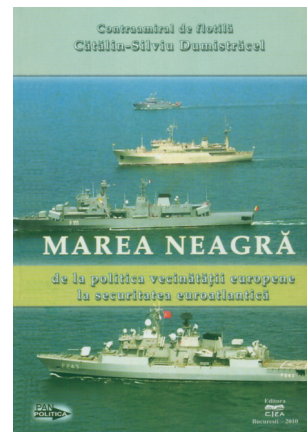
National Military Library



EDITORIAL EVENTS

 **Alina PAPOI**

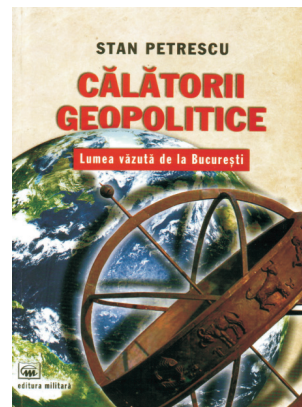
Marea Neagră de la politica vecinătății europene la securitatea euroatlantică (The Black Sea from the European Neighbourhood Policy to Euro-Atlantic Security), printed at the Publishing House of the Armed Forces Technical-Editorial Centre, under the aegis of the “Admirals Club”, “proves to be an extremely useful tool in the attempt to built an accurate and complete image of the actors in this area, their aspirations, interests, and motivations, as well as the determination of Romania’s position and especially its function in the complex mechanism that may bring and maintain stability and security in this region linked to the Balkans, Central Asia and the Middle East, in which the political, economic and security interests of some important global actors interfere and overlap, sometimes randomly, other times guided, with the ones of the Black Sea littoral states”. This words belong to Vice-Admiral (ret.) Constantin Iordache, the one who signs the foreword of the book and points out the role of the author’s research activity, concretised in this publication.



Thus, **Fleet Rear-Admiral Cătălin-Silviu Dumitrăcel** addresses the Black Sea security issue in the context of the international political scene, against the background of certain fundamental geopolitical and geostrategic changes in which there are involved actors with global vocation – the US, NATO, the EU, the Russian Federation. In this respect, there are highlighted the main geopolitical and geostrategic developments at the Black Sea, an area subject to deep changes related to two aspects: the impact of NATO enlargement on the region and the development of the cooperation between the littoral states.

The solutions to security problems in this area should be, according to the author, “sought and, above all, discussed, in the first place, by the states in this geopolitical space”. Also in this space, continues the author, Romania “must become one of the regional actors that are willing and able to transfer security and stability, as a member of NATO and the EU, to some countries that are in the transition period or which have expressed a desire for accession to these organisations”.

“If we could travel to all locations suggested by the geopolitical map, we would have the chance to taste the fruit of these <geopolitical trips> taken: we would know, study, assimilate, understand, intervene”. An invitation to reading and study – ***Călătorii geopolitice – lumea văzută de la București*** (*Geopolitical Trips – The World Seen from Bucharest*) – starts from the complexity of the current global and regional security environment. The author, **Brigadier General (r.) Prof. Dr Stan Petrescu**, encourages us to discover those connections between individuals, societies, nations, states, alliances of states, human and economic habitats, relations of forces and assets, which often do not draw our attention with something in particular. Yet, the geopolitical tool is precisely for that: to interpret the meaning of history – *“sinuous, with lights and shadows, which will never end”*, to find an explanation, if not a solution, for the main issues that challenge the life of the planet: pandemics, AIDS, acid rain, marine and land pollution, global warming, migration and, last but not least, to provide a panorama of the geopolitical maps, in the context in which they manage to make the *“impossible compromise between science, art, economics, politics (...), configuring the mathematical conjugation of worlds, civilisations, expression of economic, social and geopolitical phenomena, with the beauty and suppleness of the lines, shapes, colour tones, so that the geopolitical map of the world could be sometimes so fascinating and other times could lead us to deep reflections”*.



In terms of structure, the book addresses the state – as a key actor in the international security environment; the global and European geopolitical and geostrategic framework; the emergence of Russia and its fight against terrorism; the Caucasus-Black Sea-Mediterranean Sea region; the antimissile shield; the origin of Indians; the Arab-Israeli conflicts; the non-traditional energy resources; the unification of the Arabian Peninsula by the Saudis; the situation of the Palestinian Authority; the Six-Day War and the Fatah; the nuclear mechanism from the Central Asian corridor; the diversification of suppliers in South America; the role of mass-media in enhancing the visibility of terrorism; the wealth and the poor of the world; the water issue in the Syrian-Jordanian relations; the *Cold War* in the Arctic and the labyrinths of the Russian policy. Therefore, let us receive the author’s invitation and try *“to see the world from Bucharest !”*.

The book appeared in an excellent presentation, at the *Military Publishing House*.

*

“Today, the region in the east of the Black Sea is likely to play an important role in the European development and cooperation system. This role is prefigured by the need to transport oil and natural gas from the Caspian Sea to European consumers, as long as



the European Union has difficulties in providing energy resources. The energy crisis has proved that the peoples of Transcaucasia are interdependent because of the geographical position of the territories they occupy, in a relatively closed space, which has a huge geopolitical and geostrategic importance, and the current financial crisis confirms this". **Fleet Rear-Admiral (r.) Dr Marius Hanganu** and **Captain (r.) Ion Stan** write about the causes, circumstances or reasons that have generated a series of internal changes in the South Caucasus region, in the three countries – Armenia, Azerbaijan and Georgia, included,

“as in a vise, between the three regional powers – Turkey, Iran and the Russian Federation”, in their book ***Transcaucazia în ecuația securității din zona Mării Negre (Transcaucasia in the Security Equation at the Black Sea)***.

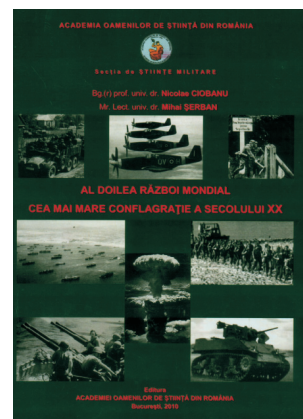
The authors analyse the risks and threats to regional security and stability from the perspective of the geopolitical and geostrategic aspects of the Wider Black Sea Region, the political-military relations and the regional security specific to the Caucasian space, the influence of the Russian-Georgian war on the economic and political-military ties in the east of the Black Sea. Last, but not least, the authors pay particular attention to Romania’s role in providing a climate of confidence and security at the Black Sea, in the development of political and military, economic and cultural relations between our country and the countries at the Eastern Black Sea.

The book, published at the *Armed Forces Technical-Editorial Centre*, was nominated for the *First Award of the Gândirea militară românească* Journal.

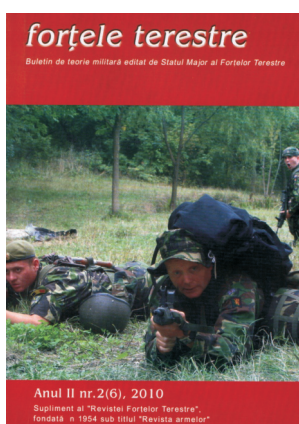
*

Under the auspices of the *Military Science Section of the Romania Academy of Scientists*, we signal the appearance of ***Al Doilea Război Mondial – cea mai mare conflagrație a secolului XX (The Second World War – The Greatest Conflagration of the 20th Century)***. The authors – **Brigadier General (r.) Dr Nicolae Ciobanu** and **Major Dr Mihai Șerban** – dedicate this book to “the 65 years since the end of this devastating scourge, which was generated by people”, wishing “to provide the readers with an overview, a compendium of this world conflict, given that the time the reader who is eager to learn what the Second World War meant is nowadays limited”. The authors succinctly present the preliminaries of war and the main military actions, grouped chronologically into three periods: the first period, from the beginning of the war until early 1943; the second period, until the second half of 1944 and the third period – the years 1944-1945, until the end of the war, on 9 May 1945, respectively 2 September 1945.

I will only give you the conclusions of this work, encouraging you, I believe, to browse these pages of history: the war lasted 2 191 days, involving over three quarters of the world population, the operations taking place on the territories of 40 countries in Europe, Asia and Africa. Among these, Europe was the most affected. The total number of the mobilised persons was of 110 million people, and the number of victims amounted to around 50 million: *“War did not solve any of the vital problems of humankind. Shortly after the Second World War, the world was divided into two big political systems with different political-military targets, the <Cold War> starting between the two camps, which lasted, in turn, more than four decades, bringing great suffering to the people who remained under the influence of the Soviet regime, representing the socialist <camp>”.*



*



Here are a few titles of the articles of the second edition of **Forțele Terestre (Land Forces)**, supplement of **Revista Forțelor Terestre (Land Forces Review)**: *“Servant leadership, the modern form of transactional and transformational leadership”*; *“The single application”*; *“Special operations forces – an overview”*; *“Terrorism and the Third World”*; *“European Gendarmerie Force – security instrument of the European Union”*; *“Diplomats of defence in the strengthening of international security and stability”*; *“Church and secularisation”*; *“The action of conventional means of destruction on military constructions”*; *“The Romanian tank – a history”*.

I suggest we stop for a moment on a paragraph in this issue: *“transformational leadership, through the clever use of inspiration, communication and understanding of the human behaviour, can motivate subordinates to achieve more than one might normally expect from them. This type of leadership plays an important role in peacekeeping missions, in which subordinates seem to be frequently consulted in determining the tasks to be accomplished. Leaders are disciplined people, who devote a part of their lives to the organisation of their own activity and of the one of the other members of the group, organisation, human community”.*

*Happy New Year
to our collaborators and readers !*

English version by
✍️ **Iulia NĂSTASIE**

THE 2009
GÂNDIREA MILITARĂ ROMÂNEASCĂ
JOURNAL AWARDS
THE 12TH EDITION – 11 November 2010

Taking place as part of the events celebrating the Day of the Romanian Armed Forces General Staff (12 November), the 12th edition of the *Gândirea militară românească* Awards was, just as in the previous years, one of the fundamental moments in the history of this publication, through which the intellectual activity in the field of military theory and science of over 50 authors was recognised and rewarded. At the opening of the ceremony, the chairman of the *Journal Awards Selection, Evaluation and Nomination Commission*, Major General Dr Virgil Bălăceanu, reviewed the work of the Commission, pointing out the importance of the 46 works selected.



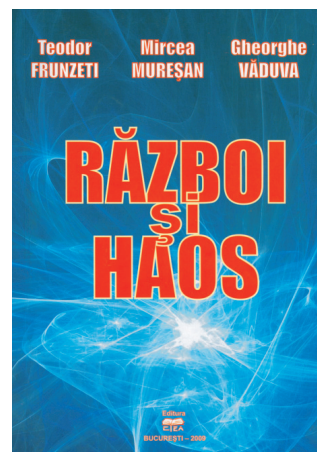
The “GMR” Journal Awards

Here are the laureates of the *Journal Awards* for this year:

- *The First Award*

of the Gândirea militară românească Journal
was given

to **Lieutenant General Dr Teodor FRUNZETI,**
General (r.) Dr Mircea MUREȘAN
and **Brigadier General (r.)**
Dr Gheorghe VĂDUVA,
for “*Război și haos*” (“*War and Chaos*”).



- *The Second Award*

of the Gândirea militară românească Journal
was given

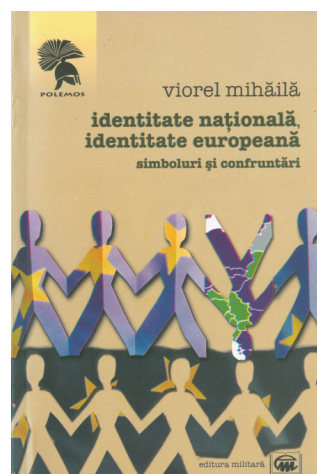
to **Major General Dr Dan GHICA-RADU**
and **Colonel Dr Adrian TONEA**
for “*Influența mediului operațional asupra*
modalităților de utilizare a puterii militare
pentru gestionarea conflictelor în epoca globalizării”
 (“*The Influence of Operational Environment*
on the Ways of Using Military Power for Conflict
Management in the Age of Globalisation”).



- *The Third Award*

of the Gândirea militară românească Journal
was given

to **Viorel MIHĂILĂ**
for “*Identitate națională, identitate europeană.*
Simboluri și confruntări”
 (“*National Identity, European Identity.*
Symbols and Confrontations”).



Other nominees for the Gândirea militară românească Journal Awards were:

Nominees for the **First Award:**
“Noul aliat. Regândirea politicii de apărare a României la începutul secolului XXI”
 (“The New Ally. Rethinking Romania’s Defence Policy at the Beginning of the 21st Century”),
author **Dr George Cristian MAIOR**,
and “Transcaucazia în ecuația securității din zona Mării Negre” (“Transcaucasia in the Security Equation at the Black Sea”),
author **Fleet Rear-Admiral (r.) Dr. Marius HANGANU**
and **Captain (r.) Ion STAN**.



Nominees for the **Second Award:**
“Operația contrateroristă”
 (“Counterterrorist Operation”),
authors **General (r.) Dr Eugen BĂDĂLAN**
and **Colonel Dr Vasile BOGDAN**,
and “Acțiunile sistemului artileriei terestre pe timpul ducerii operației de apărare”
 (“Actions of Land Artillery during Defence Operations”),
author **Brigadier General Dr Florinel DAMIAN**.

Nominees for the **Third Award:**
“Despre lovitura de stat și apărarea împotriva ei” (“On Coup d’état and Defending against It”),
author **Air Flotilla General Dr Victor STRÂMBEANU**,
and “Regiunea extinsă a Mării Negre. Delimitări teoretice și practice ale unui areal geopolitic în plină redefinire”
 (“The Wider Black Sea Region. Theoretical and Practical Delimitations of a Geopolitical Area in Full Redefinition Process”),
coordinator **Major General (r.) Dr Mihail E. IONESCU**.



There were also given three Certificates of Excellence, as follows:

- to **Colonel (r.) Dr Petre OTU** for *„Mareşalul Alexandru Averescu. Militarul, omul politic, legenda”* (*“Marshall Alexandru Averescu. The Soldier, the Politician, the Legend”*), a special contribution to the development of the theoretical heritage of the national military science;



- to the **Armed Forces Historical Service**, for the works published for the celebration of 150 years since the General Staff was established: *“Enciclopedia Armatei României”* (*“The Romanian Armed Forces Encyclopaedia”*), *“Albumul Armatei României”* (*“The Romanian Armed Forces Album”*) and *“Statul Major General în arhitectura organismului militar românesc. 1859-2009”* (*“The General Staff in the Architecture of the Romanian Military Body. 1859-2009”*);

- to the **Armed Forces Technical-Editorial Centre** for the works published for the celebration of 150 years since the General Staff was established.

GMR



2010 / 2011

Thank you, dear collaborators, for the word materialised in the pages of the journal of the General Staff!

Thank you for the fact that, together, we have written a page in the history of the Romanian Military Thinking!

Therefore, it is to each of You we express our gratitude and appreciation:

1. Colonel Călin ALMĂȘAN
2. Brigadier General (r.)
Dr Constantin APETROAIE
3. Colonel Adrian BĂLĂLĂU
4. Colonel Nicu BEGANU
5. Commander
Dr Gheorghe-Cristian BOGDAN
6. Major General Dr Fănică CĂRNU
7. Dr Erdal CAYIRCI
8. Captain Dr Constantin CIOROBEA
9. Lieutenant Colonel Petrică CRAIOVEANU
10. Dr Irina CUCU
11. Lieutenant Colonel Victor DĂNILĂ
12. Colonel Gheorghe DIMA
13. Colonel Dr Gheorghe DINCĂ
14. Fleet Rear Admiral
Cătălin Silviu DUMISTRĂCEL
15. Dr Petre DUȚU
16. Commander Brian FINMAN
17. Lieutenant Colonel Ovidiu-Stelian FIZEȘAN
18. Luminița GIURGIU
19. Commander
Dr Olimpiu Manuel GLODARENCO
20. Commander Claudiu GROSU
21. Dr Jeffrey HUNKER
22. Captain Constantin IFRIM
23. Colonel BEng Teodor INCICAȘ
24. Lieutenant General Dr Sorin IOAN
25. Colonel Dr Crăișor-Constantin IONIȚĂ
26. University Assistant
Anelis-Vanina ISTRĂTESCU
27. Colonel Dr Florin LĂPUȘNEANU
28. Colonel (r.) Eugen LUNGU
29. Colonel Dr Liviu Marilen LUNGULESCU
30. Colonel Vasile MAIER
31. Dr Tamara MAKARENKO
32. Lieutenant Colonel Dr Eugen MAVRIȘ
33. Prof. Dr Jing MEN
34. Lieutenant Commander
Laurențiu MEȘTERCA
35. Petrică MIHALACHE
36. Colonel Leonard MOCANU
37. General (r.) Dr Mihail ORZEATĂ
38. Colonel Relu PANAIT
39. Gretchen PETERS
40. Delia PETRACHE

- | | |
|---|---|
| 41. Colonel Daniel PETRESCU | 51. Colonel Dr Mihai ȘTIR |
| 42. Lieutenant Colonel Dr Virgil Ovidiu POP | 52. Brigadier General
Tomiță Cătălin TOMESCU |
| 43. Dr Mihai POPESCU | |
| 44. Lieutenant Colonel Ștefan PREDA | 53. Michito TSURUOKA |
| 45. Colonel Mihai RADU | 54. Colonel (r.) Dr Florentin UDREA |
| 46. Lieutenant Colonel Filofteia REPEZ | 55. Lieutenant Colonel Valentin VASILE |
| 47. Cătălina ROJIȘTEANU | 56. Colonel Veronel VAVURĂ |
| 48. David SNOWDON | 57. Commander BEng Adrian VOINEA |
| 49. Dr Florin STAN | 58. Major General Dr Cătălin ZISU |
| 50. Major General Alojz ŠTEINER | 59. Andreea C. ZUGRAVU |

“RMT” Editorial Staff



Résumés

Sécurité par coopération

Grâce à son nouveau Concept stratégique adopté lors du récent Sommet de Lisbonne, l'OTAN a réaffirmé sa cohésion et la solidarité du monde occidental sur la feuille de route par l'Alliance à répondre efficacement aux défis du XXI^e siècle, en vertu de l'obligation de confirmer le statut de pilier de la sécurité mondiale et, bien sûr, pour approprier le titre d'avoir le mieux réussi au monde. L'Alliance renforce et réaffirme son partenariat avec l'Union européenne, une autre institution par qu'elle est exprimée la sécurité, mais en même temps l'OTAN se déclare pour la politique des portes ouvertes et elle s'engage à développer de nouvelles capacités et de nouveaux partenariats.

La guerre continue – le milieu de confrontation (II)

Les multiples dimensions de la confrontation exigent que tous les décideurs, en particulier les militaires, doivent étudier très bien l'environnement avant toute décision et action. Le cyberspace, l'espace aérien et l'espace cosmique permettent l'existence d'un milieu de confrontation. Dans le cyberspace existent des réseaux des communications et des ordinateurs qui utilisent des produits informatiques qui sont envoyés et reçus par des moyens physiques et électromagnétiques. Le temps, les forces opposées et l'espace sont les facteurs les plus importants qui opèrent sur les actions militaires pendant la guerre.

La conception d'un soutien logistique de l'OTAN dans les opérations de réponse aux crises

Le soutien logistique de l'OTAN dans les opérations de réponse aux crises est basé sur le potentiel logistique des Etats participants et aussi par l'équilibre dans l'équation responsabilité collective – responsabilité nationale. Dans cette perspective, la mise en œuvre des solutions multinationales peuvent générer une répartition plus précise des ressources et accroître l'efficacité dans le fonctionnement de la logistique.

Au cours de la participation à des opérations militaires de réaction aux crises, le soutien logistique est en cours d'exécution en vertu des dispositions du commandant d'un échelon stratégique ou opérationnelle, qui dirige l'opération.

La transformation des organisations militaires – particularités de la transformation de l'Armée Roumaine dans le contexte de son intégration européenne et euro-atlantique (II)

Au début du ce millénium, le monde est entré dans une nouvelle phase du développement marquée par la coexistence et la confrontation des tendances positives avec d'autres

qui génèrent des risques majeurs et aussi des menaces. Sous l'influence des changements dans l'environnement de sécurité, de la nouvelle forme d'expression des risques spécifiques et les menaces, la transformation de la structure des forces armées roumaines est un processus naturel, qui permettra l'organisation et la préparation des forces pour la participation à la défense nationale et collective, pour l'amélioration de la capacité pour la gamme complète d'actions, pour la lutte contre le terrorisme et l'accomplissement d'autres tâches qui lui sont assignées.

Le Jihad et la dynamique de la sécurité mondiale

L'auteur commence par une brève introduction sur la nouvelle tendance pour en relier avec le monde islamique, notant un élément qui a fourni à la nouvelle administration américaine une crédibilité accrue: l'élimination du syntagme «*guerre contre le terrorisme*».

Puis, il fait une tentative à «*déchiffrer*» le djihad – une des plus concepts importants de l'Islam. En outre, il adopte une approche à certains religieux, idéologiques, aspects militaires et politiques concernant ce concept.

En fin de compte, il tire quelques conclusions du point de vue de l'influence du «*jihad offensif*».

Combattre la piraterie au large de côtes somaliennes – la dimension maritime

L'article se concentre sur la réponse de la communauté maritime au sujet de la piraterie somalienne. Il décrit les efforts entreprises par les organisations civiles et militaires et souligne les mesures anti-piratage prises par les commerçants que la première ligne de la défense. Il décrit aussi le rôle des forces de la marine dans la lutte contre le piratage,

ce qui reflète la controverse autour de la pratique de l'utilisation de navires de guerre dans cette mission. Après avoir présenté les acteurs concernés, l'auteur explique l'évolution de la lutte contre la piraterie, les tactiques utilisées par des forces navales, ainsi que les défis qui nous attendent.

Provocations de sécurité via l'Internet

Aujourd'hui, l'environnement de sécurité doit face à plusieurs défis (des risques et des menaces à la sécurité). Ceux-ci occupent un rôle central: le terrorisme international, la prolifération des armes de destruction massive, les conflits froids, la criminalité organisée. Pour cela maintenant on ajoute les problèmes de sécurité provenant de cyberspace via Internet.

A cet égard comprennent: le cyber terrorisme, la cybercriminalité, les documents produits par les pirates. Par conséquent, l'environnement de sécurité actuel comprend à la fois l'espace réel et le cyberspace. De plus en plus, on remarque l'influence et le potentiel de l'Internet dans les différentes sphères de l'activité humaine aux niveaux local, national, régional et mondial.

Tendances dans l'évolution du soutien logistique dans les conflits de la future

L'OTAN et les Etats membres sont sur le bord d'une nouvelle transformation générée par le Nouveau concept stratégique, ainsi qu'en raison de l'engagement dans le défi des opérations de ce millénium, telles que la FIAS. Sur la base de certains hypothèses, telles que: l'OTAN restera plus de 10 ans en Afghanistan ou les modèles lancés par les opérations en Iraq ou en Afghanistan

ne peuvent pas être universelles, nous pouvons tirer les principaux tendances en ce qui concerne les évolutions dans le domaine de le soutien logistique pour les conflits futurs, en envisageant les 10-15 prochaines années.

Certaines opinions à l'égard d'un possible système intégré de management de renseignements qui se réfèrent à l'instruction dans le domaine des communications et de l'informatique (II)

L'objectif général d'une information intégrée d'un système de gestion est de maintenir un système efficient de formation qui répond aux besoins de l'Alliance. Un tel système devrait lier la formation de l'unité aux exigences de la mission, en fournissant dans le même temps les outils nécessaires pour l'évaluation de formation en unité. Une structure de communication qui a effectué des missions dans le théâtre des opérations a une expérience opérationnelle qui lui permet d'aborder le processus de formation avec un niveau de compréhension aux réalités spécifiques du présent et l'avenir dans le domaine dans lequel elle procède.

Les défis économiques et sociaux de la sécurité internationale

Au début, l'auteur présente les nouveaux types de conflits, les questions économiques, qui ne pas déclencher la perte directe de la vie, et pourtant faire plus «*victimes collatéraux*». Ensuite, elle écrit que l'expérience de plus récents conflits dans le monde montre que, après l'échec de la diplomatie et de la diplomatie coercitive, affirme souvent recourir à d'autres instruments du pouvoir: de l'information, économiques et militaires. En outre, elle mentionne que les conflits non seulement détruisent

les infrastructures, mais aussi encouragent le crime, encombrant les investissements et rendent impossibles les activités économiques normales.

La guerre cybernétique et la pouvoir cybernétique. Problèmes de la doctrine de l'OTAN

Dans cet article de la recherche, l'auteur met l'accent sur certains termes très utilisés dans le débat actuel de la sécurité internationale, et aussi dans les discussions au sujet du nouveau concept stratégique de l'OTAN, ainsi: cyber espace, cyber menaces, les attaques cybernétiques, les cyber terrorisme et la pouvoir cybernétique.

En ce sens, l'auteur définit les types d'attaques cybernétiques, ainsi que les concepts de guerre cybernétique et de la pouvoir cybernétique. Ensuite, il écrit sur le nombre de défis posés par l'utilisation du pouvoir de la cybernétique.

Les fédérations multi résolution dans l'appui des opérations assistant par l'ordinateur du niveau opérationnel et supérieur

Les fédérations multi résolution sont encore à leur commencement. Leur utilité est souvent discutée et il y a une telle confusion quant à la taxonomie connexe. Dans cet article, tout d'abord sont expliquées les définitions pour le champ et elles sont clarifiées, et aussi les derniers développements. Puis, sont expliquées les avantages des fédérations multi résolution par d'exercices assistés par l'ordinateur, à l'aide d'un exemple vignette.

Dans les opérations militaires, la simulation est utilisée à des fins diverses, tels que le développement des capacités, la planification de la défense, le soutien à l'exploitation et de la formation.

**European Think Tanks:
Regional and Trans-Atlantic Trends
– report of The Think Tanks
and Civil Societies
Program 2009 (IV)**

Cette étude se propose à examiner tous les groupes de réflexion au sein de l'Union européenne de juin 2009, en présentant quelques-unes des principales tendances et défis auxquels ils sont confrontés.

L'auteur estime que leurs rôles dans la société civile n'ont jamais été aussi grands, compte tenu de la crise économique actuelle, quand leurs idées et leurs recommandations sont les plus nécessaires.

Voici le final part de cette étude, dans lequel l'auteur présente les dernières think tanks européens.

**Repérés historiques des Forces
Navales Roumaines**

Les auteurs soulignent l'importance des forces navales roumaines dans la conception de la Roumanie au sujet de son système de défense nationale. Tout d'abord, ils écrivent sur les tâches de la marine roumaine pendant la guerre d'indépendance (1877-1878). Ensuite, ils mentionnent la vaste gamme de missions que la marine roumaine a afin de couvrir au cours de la Première Guerre mondiale et la guerre de l'unification nationale. En outre, ils prennent une approche à la doctrine navale pendant les deux guerres mondiales, en mettant l'accent sur les programmes de modernisation de la Marine roumaine au cours des années 1918 et 1941 et les actions navales au cours de la Seconde Guerre mondiale.

Version française par Alina PAPOI

The editorial and layout process
was completed on 8 December 2010.



*We thank you all – the collaborators and readers
of our journal alike, and we wish you happy holidays.*

May you be healthy and loved !

Happy New Year !

**Cover 1: Military Parade organised in the Arch of Triumph Square – 1 December 2010, București.
Photo – Petrică MIHALACHE**

**Cover 4: Ceremony organised at the Tomb of the Unknown Soldier in Carol Park
– 1 December 2010, București. Photo – Petrică MIHALACHE**



<http://www.defense.ro/gmr>