



1 January
March
2013

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, 9th year -**

Romanian Military Thinking



PUBLISHER

ROMANIAN ARMED FORCES

GENERAL STAFF

EDITORIAL BOARD

CHAIRMAN

Lt Gen Dr Dan GHICA-RADU

MEMBERS

Academician Dan BERINDEI

Lt Gen Dr Teodor FRUNZETI

Lt Gen Dr Sorin IOAN

Lt Gen (AF) Dr CĂRNU Fănică

Lt Gen (N) Dr Aurel POPA

Maj Gen Dr Avram CĂTĂNICI

Maj Gen Alexandru RUS

Brig Gen (AF) Dr Florian RĂPAN

Brig Gen Dr Gheorghe MOTOC

Col Dr Mircea TĂNASE

SCIENTIFIC REVIEWERS

Gen (r.) Dr Mihail ORZEAȚĂ

Brig Gen (r.) Dr Costică ȚENU

Col Dr Ion ROCEANU

Col (r.) Dr Ion GIURCĂ

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

110 Izvor Street, Sector 5, Bucharest

Postal code: 050564

Telephone: +4021.410.40.40/1001731; 1001732

Tel/Fax: +4021.319.56.63

<http://www.mapn.ro/smg/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.

Romanian Military Thinking
is a scientific journal with acknowledged prestige
in the field of "Military Science, Information
and Public Order", in keeping with the evaluation
carried out by the National Council
for Titles, Diplomas and Certificates (CNATDCU)
in 2011

(<http://www.cnatdcu.ro/wp-content/uploads/2011/11/reviste-militare1.pdf>)

1 January
March
2013

Romanian Military Thinking

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

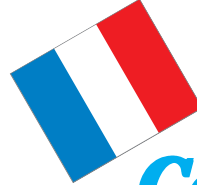
Founded in 1864 under the name "Military Romania"
- English edition, 9th year -

*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 included in the Journal Master List
of the Index Copernicus International database*



Contents



Contenu

Editorial

Intelligence for Security
Colonel Dr Mircea TĂNASE

Editorial

7 Intelligence pour sécurité
Colonel dr. Mircea TĂNASE

Conceptual Projections

NATO Bodies Responsible
for the Reserve Forces Establishment,
Employment, Command and Control
Colonel Adrian BĂLĂLĂU

Projections conceptuelles

1 1 Des organismes de l'OTAN
avec les responsabilités de créer,
utiliser, commander et contrôler
les forces de réserve
Colonel Adrian BĂLĂLĂU

Demands on National Operational
Communications Systems
for their Integration
into Unified Communications Systems
in Coalition Operations
Colonel Daniel BRĂTULESCU

2 3 Exigences des systèmes
de communications opérationnels
nationales d'intégrer les systèmes
de communications unifiées
dans les opérations de coalition
Colonel Daniel BRĂTULESCU

Intelligence Culture

Information Warfare
between Threat and Force Multiplier
Fleet Rear Admiral (N)
Dr Cătălin-Silviu DUMISTRĂCEL

La culture d'intelligence

3 3 La guerre de l'information
entre la menace et le multiplicateur
de puissance
Contre-amiral de la flottille (MN)
dr. Cătălin-Silviu DUMISTRĂCEL

- | | |
|---|---|
| <p>Intelligence – Coordinate of National and Global Security Equation
<i>Colonel Ovidiu FRĂȚILĂ</i>
<i>Lieutenant Colonel Iosif SOLOMON</i></p> | <p>4 2 Intelligence – une approche coordonnée de l'équation de la sécurité nationale et mondiale
<i>Colonel Ovidiu FRĂȚILĂ</i>
<i>Lieutenant-colonel Iosif SOLOMON</i></p> |
| <p>Intelligence Services and Early Warning
<i>Lieutenant Colonel Cătălin BALOG</i></p> | <p>5 6 Les services d'intelligence et l'alerte avancée
<i>Lieutenant-colonel Cătălin BALOG</i></p> |
| <p>Open Source Intelligence – Opportunities to Support and Develop High-Performance and Effective Education System in the Defence Intelligence Field
<i>Colonel Dr Cristian-Victor CIȘMIGIU</i></p> | <p>6 8 Les sources ouvertes d'information – possibilités de soutenir et développer pour une formation performante et efficace dans le domaine des informations pour la défense
<i>Colonel dr. Cristian-Victor CIȘMIGIU</i></p> |
| <div style="display: flex; justify-content: space-around; margin: 10px 0;"><div style="background-color: #ADD8E6; padding: 5px 20px; border-radius: 10px;"><i>Opinions</i></div><div style="background-color: #ADD8E6; padding: 5px 20px; border-radius: 10px;"><i>Opinions</i></div></div> | |
| <p>Airpower in the Asymmetrical Conflict. Case Study: Afghanistan (II)
<i>Major General (AF)</i>
<i>Dr Victor STRÎMBEANU</i></p> | <p>7 7 La puissance aérienne dans un conflit asymétrique. Étude de cas: l'Afghanistan (II)
<i>Major-général (AA)</i>
<i>dr. Victor STRÎMBEANU</i></p> |
| <p>Psychological Selection to Join the Military System in the Light of the Model of Multiple Intelligences
<i>Colonel Dr Adrian PRISĂCARU</i></p> | <p>8 7 La sélection psychologique pour accéder dans le système militaire par l'intermédiaire du modèle des intelligences multiples
<i>Colonel dr. Adrian PRISĂCARU</i></p> |
| <p>Space as Military Environment – Between Law and Power
<i>Lieutenant Colonel Dorian LUPARU</i></p> | <p>1 0 3 L'espace comme un environnement militaire – entre la loi et la puissance
<i>Lieutenant-colonel Dorian LUPARU</i></p> |

*Neopolitics • Neostrategy
International Security*

*Néopolitique • Néostratégie
Sécurité internationale*

The People's Republic of China
Cyber Capabilities
Major Marian LAZĂR

1 1 8 Les capacités cybernétiques
de la République Populaire de Chine
Commandant Marian LAZĂR

Security Strategies in Certain
EU Member States.
The Case of Spain
Dr Tiberiu TĂNASE

1 2 3 Stratégies de sécurité dans certains
Etats membres de l'UE.
La case de l'Espagne
Dr. Tiberiu TĂNASE

*International
Connections*

*Connexions
internationales*

NATO Enlargement Reloaded
Karl-Heinz KAMP

1 3 6 Le nouvel élargissement de l'OTAN
Karl-Heinz KAMP

Securing the Sahel: A Role for NATO?
Paul PRYCE

1 4 7 Sécurisation du Sahel: un rôle
pour l'OTAN ?
Paul PRYCE

NATO's Dealing
with a Different Gulf Now
Jean-Loup SAMAAAN

1 5 1 L'OTAN a aujourd'hui affaire
à un Golfe différent
Jean-Loup SAMAAAN

*Round-Table
Discussions*

*Table
ronde*

Capability Identification, Planning
and Development
in the Romanian Armed Forces
Captain (N)

Theodor Nicolae ENACHE

1 5 7 L'identification, la planification
et le développement des capacités
de l'Armée Roumaine
Colonel (MN)

Theodor Nicolae ENACHE

- Confidence and Security Building in the Wider Black Sea Region through Multinational Cooperation within Smart Defence and Pooling & Sharing Initiatives
Captain (N) Vicențiu CĂTĂNEANU
- 160 L'augmentation de la sécurité et de la confiance dans la zone élargie de la Mer Noire par la coopération multinationale des initiatives Smart Defence et Pooling & Sharing
Colonel (MN) Vicențiu CĂTĂNEANU

Pages of Military History

Pages de l'histoire militaire

- French Geopolitics in the Far East in the Second Half of the 19th Century
Captain (N) Dr Olimpiu Manuel GLODARENCO
Captain (N) Ionel Dan CIOCOIU
- 167 La géopolitique française en Extrême-Orient dans la seconde moitié du XIX^e siècle
Colonel (MN) dr. Olimpiu-Manuel GLODARENCO
Colonel (MN) Dan CIOCOIU

- The "Secrets" of the Success on the Secret Front
Colonel Daniel MELCIOIU
- 179 Les „Secrets“ du succès sur le Front Secret
Colonel Daniel MELCIOIU

Military Journalistic Universe

195 *Univers journalistique militaire*

Intelligence for Security

Ensuring national security is vital to the existence and proper functioning of any society, and intelligence services play a key role in this process.

Information, this “*talisman of power*”, as someone wonderfully said, is sought at all the levels of the global social system, a *sine qua non* in any field of human activity, and especially in the military, where *intelligence* is defined as information meant for action.

Security and *intelligence* are two terms that are present today more than ever in both political discourse and public opinion due to the change of attitude and reconsideration of these domains following the turning point in September 2001.

The state, as the main security generator of the nation, needs the services provided by *intelligence* more than ever, its actional result being certainly determined by its functional dimension.

Today, when over democratic societies looms not only the threat of foreign military aggression but also the risks related to terrorism, organised crime, illegal trafficking in human beings, weapons and other goods, and the development of some regional conflicts, *intelligence* services should consider the new features of the information society and redefine their objectives, strategies and doctrines to perform the fundamental role of collecting and analysing information regarding these possible threats as well as that of assessing risks.

Information, in whatever form, is part of the arsenal of new asymmetrical conflicts, and the social recognition of the usefulness of *intelligence* does not need to be proven. However, it should be remodelled to meet the new characteristics of the security environment that is increasingly complex and unpredictable. That is why it is necessary to reconsider the role and weight of *intelligence* services in the decision-making process – the indissoluble link between *intelligence* and decision –, the quantity and quality of its products supporting a political action in favour of the fundamental interests of the state.

Whether they represent a form of the state power or, as stated by other theorists, only a means that is necessary to exercise it, having *intelligence* services and engaging them in an effective manner represent the key to success in identifying these new forms of threat as well as the methods to prevent them.

Even if there is no reverse projection of security values, more often than not, the nation is not aware of the success of *intelligence* and of its contribution to the nation stability and security, but it is very sensitive to and affected by *information failures*, with unpredictable effects on the political, social and even economic aspects.

Intelligence culture, a new syntagm that has gained authority in everyday life lately, finds its expression, in the military, as a complex of norms, concepts, values, traditions, beliefs and ethical practices that help preparing the military personnel to effectively use information and information products in exercising own prerogatives.

Certainly, *intelligence culture*, understood and accepted in the broader context of *security culture*, can be achieved only through proper education and training, employing methods that are appropriate to the intended goals and standards. In this context, defence intelligence education, a domain having a long tradition, continuous evolution and remarkable regeneration potential, configured for an optimal didactic interaction, has succeeded in providing complex and effective educational services. Specific educational institutions, permanently impregnated with the attribute of modernity, are currently adapted to meet the requirements related to the education and professional development of experts in this field of activity. The desire to stand out, to have a high status, and to achieve academic recognition within the Romanian military education system represents only natural and justified aspirations that are certainly supported by the results achieved under the imperative of providing highly professionalised *end products*, capable of meeting the increasingly complex requirements in the current context that is strongly marked by profound paradigm shifts in national and international security.

 *Colonel Dr Mircea TĂNASE*

English version by
Diana Cristiana LUPU

Intelligence pour sécurité

Assurer la sécurité nationale est indispensable à l'existence et au fonctionnement normal de toute société et les renseignements jouent un rôle essentiel dans ce processus.

L'information, ce „*talisman du pouvoir*“, comme quelqu'un l'a bien exprimé, est demandée à tous les niveaux du système social global, une condition *sine qua non* dans tous les domaines de l'activité humaine. Et surtout dans le domaine militaire, où *l'intelligence* est définie comme une information destinée pour l'action.

Sécurité et *intelligence*, voici deux mots qui sont présents aujourd'hui plus que jamais, à la fois dans le discours politique et dans l'opinion publique, en raison du changement d'attitude et d'une nouvelle considération de ces domaines après le tournant de septembre 2001.

L'État, en tant que principal entité de sécurité de la nation, a besoin plus que jamais des services *d'intelligence*, et ses résultats concrets étant certainement dûs par sa dimension fonctionnelle.

Aujourd'hui, quand les sociétés démocratiques sont menacées pas certainement d'une agression militaire étrangère, mais surtout des risques de terrorisme, de la crime organisée, du trafic illégal de personnes, d'armes et d'autres marchandises, ainsi que le développement des conflits régionaux, les services *d'intelligence* doivent tenir compte de nouvelles caractéristiques de la société de l'information et de redéfinir ses objectifs, ses stratégies et ses doctrines pour exercer son rôle fondamental de recueillir et d'analyser des informations sur ces possibles menaces et aussi de l'évaluation des risques.

L'information, sous quelque configuration propre, fait partie de l'arsenal de nouveaux conflits asymétriques et la reconnaissance sociale de l'utilité de *l'intelligence* ne pas doit prouvée, mais il est présente la question de sa renaissance sur les nouvelles caractéristiques de l'environnement de sécurité, de plus en plus complexe et imprévisible. C'est pourquoi il est nécessaire de reconsidérer le rôle et l'importance des services *d'intelligence* dans la prise de décision – le lien indissoluble entre *intelligence* et décision –, la quantité et la qualité de ses produits en soutenant une action politique en faveur des intérêts fondamentaux de l'État.

L'action d'avoir et l'engagement efficient des services *d'intelligence* représentent la clé du succès dans l'identification de ces nouvelles formes de menaces et dans le moyen de les prévenir, soit que ces services sont une forme de pouvoir de l'État ou, comme il est dit par d'autres théoriciens, seulement un exercice nécessaire de sa propriété.

Même si on ne peut parler d'une projection inverse des valeurs sécuritaires, la nation, le plus souvent, n'est pas au courant des succès *d'intelligence* et de leur contribution à sa stabilité et à sa sécurité, mais elle est très sensible et affectée par *les défaillances d'information*, avec des effets imprévisibles sur les aspects politiques, sociales et même économiques.

La culture d'intelligence, une nouvelle syntagme qui s'est imposée ces derniers temps avec l'autorité dans la vie quotidienne, se manifeste dans le domaine militaire comme un ensemble de règles, concepts, valeurs, traditions, croyances et pratiques éthiques par lequel le personnel militaire est prêt pour l'utilisation efficace des informations et des produits d'information pour accomplir ses propres prérogatives.

Bien sûr, cette *culture d'intelligence*, comprise et acceptée dans l'ensemble entier de la *culture de sécurité*, ne peut être atteinte que grâce à une formation adéquate, par des méthodes appropriées aux objectifs et aux performances ciblées. Dans ce contexte, l'éducation des renseignements pour la défense, un domaine d'activité avec une longue tradition, une évolution continue et un remarquable potentiel de régénération, configurée pour une interaction didactique optimale, a conduit à obtenir des services éducatifs complexes et efficaces. Des institutions d'éducation spécifiques, toujours au courant de la modernité, sont actuellement adaptées aux exigences de formation et de perfectionnement professionnel des spécialistes dans ce domaine d'activité. Le désir d'affirmation, celle de la statuer et celle d'obtenir de la reconnaissance académique dans le domaine de l'éducation militaire roumaine ne sont que des aspirations naturelles et justifiées qui certainement sont pris en charge par les résultats obtenus sous l'impératif de fournir *des produits finis* professionnalisés dans un haut niveau, capables de faire face aux requêtes de plus en plus complexes, dans le contexte actuel, fortement marqué par de profonds changements de paradigme dans la sécurité nationale et internationale.

*Version française par
Alina PAPOI*

NATO BODIES RESPONSIBLE FOR THE RESERVE FORCES ESTABLISHMENT, EMPLOYMENT, COMMAND AND CONTROL

Colonel Adrian BĂLĂLĂU

NATO nations have undergone major transformations within their armed forces. The author considers that reserve forces are important so that the Alliance can conduct joint and combined operations and a broader spectrum of missions.

In this respect, the NRFC was established in 1981 as an independent, informal group of senior national officers responsible for reserve matters. The committee's objectives are to strengthen the Alliance reserves readiness by providing a forum for informal and candid exchange of information in areas such as mobilisation, organisation of peacetime reserve forces, motivation of reserve forces and employer support. It serves as a committee to provide policy advice on reserve issues to NATO's Military Committee. The NRFC also provides appropriate advice and support to the Interallied Confederation of Reserve Officers, to assist them in their activities in support of Alliance goals and to advise the MC on its relationship with CIOR.

Keywords: *reserve forces; Allied Command Transformation; National Reserve Forces Committee; Interallied Confederation of Reserve Officers*

The different share of reserve forces in the armies' force structure plays a decisive role as far as the level of the structures in charge of their planning is concerned. The commonality of all modern armies is that there are structures at central level, having coordination and control responsibilities, as well as execution structures, at the level of armed forces services, and all these structures with responsibilities in the field of reserve forces perform activities related to their recruitment, selection, establishment and training.

The issue of armed forces mobilisation is a purely national one, as there is neither a NATO policy nor unitary regulations in this respect. However, there are different bodies within the North Atlantic Alliance or recognised by it, which have responsibilities for the reserve forces establishment, employment, command and control.

The main tasks of these bodies are as follows: to complete the active military structures participating in NATO article 5 and non-article 5 operations, to establish voluntary reserve forces,

Colonel Adrian Bălălău – the Personnel and Mobilisation Directorate, the General Staff, the Ministry of National Defence.

to support the state institutions and/or local authorities in emergency situations, to ensure reserve forces participation in multinational structures.

The Military Committee – MC is the senior military authority in the Alliance and performs the activity under the political guidance of the North Atlantic Council, the Defence Policy and Planning Committee, and the Nuclear Planning Group, being authorised to periodically assess the need to review *NATO Military Committee Concept regarding Reserve Forces*, including the aspects related to their employment and force generation. To this end, it periodically makes recommendations to the National Reserve Forces Committee to continue to encourage the support for providing the reserve forces that are necessary in current operations and to review the policy on ensuring reserve forces.

The International Military Staff – IMS plans, evaluates and recommends policies regarding military aspects, including in the field of *reserve forces*, submits them to MC analysis, and ensures the immediate implementation of the North Atlantic Council decisions. It is staffed with permanent civilian personnel and military personnel provided by member nations on the allocation of posts.

The Allied Command Transformation – ACT provides the institutional framework for managing the transformation of NATO's capabilities. *“Transformation means to do our duty in NATO in a more intelligent way. To this end, it is necessary to focus on the future capabilities, training, education, doctrine and concepts and, especially, we must understand that the entire agenda requires a change in culture and perception”*¹.

As the engine of NATO military transformation, ACT unitarily coordinates the energies and creativity of nations, and focuses its effort to lead the Alliance forward, innovative intellectual thinking being critical in this process. One of the most important decisions has been that of changing NATO command structure to ensure *“a more flexible, effective and efficient command structure that can be easily deployed in order to meet the operational requirements necessary to carry out the full range of Alliance missions”*. In its headquarters, the same with that of the United States Joint Forces Command Norfolk, Virginia, ACT has command elements at the Joint Warfare Centre in Norway, the Joint Analysis and Lessons Learned Centre in Portugal, the Joint Force Training Centre in Poland and the Centre for Maritime Research and Experimentation in Italy. ACT is represented and supported by staff elements at NATO headquarters and SACEUR².

¹ Cf. Admiral Sir Mark Stanhope, British Royal Navy, opening speech, NRFC Winter Meeting, ACT HQ, Norfolk, 2006

² Cf. *NRFC/CIOR annual report*, presented at the NRFC Winter Meeting, ACT HQ, Norfolk, 2011.

Based on the philosophy of vertical and horizontal matrix, ACT, employing modern management methods, focuses its activity on *four functional areas* of NATO Military Transformation: capabilities; implementation; command, control, communications, computers and intelligence (C4I); resources and logistics.

In addition to the four functional areas, five *Integrated Capability Teams – ICTs* have been established to coordinate, plan, identify, analyse and advise on the solutions for the capabilities that are specific to the Transformation Areas and Goals as follows: *Information Superiority & NATO Network Enabled Capabilities; Expeditionary Operations; Integrated Logistics; Effective Engagement & Joint Manoeuvre; Enhanced CIMIC.*

ACT coordinates the educational activities within NATO School in Oberammergau and the research within the Centre for Maritime Research, La Spezia, Italy, with a view to understanding the security environment, new concepts, staff procedures, resource and capability management process and, last but not least, to experimenting and validating novel ideas and concepts, in the spirit of military transformation.

ACT has developed and maintained an active partnership with the nations, NATO agencies and training centres, national and multinational centres of excellence, academia and industry, being able to manage and coordinate military transformation as the processes, structures and relation systems are organised as business lines, which are completely different from conventional military structures and methods. This approach allows ACT to be innovative and proactive, to materialise concepts and capabilities in a deliberate and systematic manner, to assess progress, to be flexible and to cope with unpredictable or atypical aspects of the transformation process.

On the ACT server in Norfolk a restricted database has been created, providing *detailed information regarding reserve force systems*, as well as regarding the legal provisions and social facilities granted to the reservists within the nations that have contributed to the database.

Moreover, ACT provides NATO leadership and nations with expertise in the fields of military transformation. ACT structures and processes and its relations with other organisations are continually assessed and adapted to remain viable and constructive, the full range of its initiatives representing a solid foundation for facilitating the Alliance sustainable transformation.

The results of these changes are still impressive, primarily because all operational responsibilities are placed under the ACO command, thus achieving a clearer division of labour between the ACO and the newly established ACT – the former sets the standards for the units and the latter provides the necessary training

so that they could be included in a NATO command. Both certify that the standards set for these units are met.

Therefore, the main objectives of ACT are to organise NATO agenda regarding defence planning and the Alliance capabilities transformation. ACT has a rich experience that should be shared with the other Alliance member states. However, they often choose to develop their own transformation agenda without cooperating with the Alliance. There are few instances when these states may benefit from the experience of the other members with regard to defining capability requirements and planning future forces. *Moreover, they should lead to the revival of Prague Capabilities Commitment – PCC to concentrate efforts on the capability deficiencies that have an impact on NATO Response Force – NRF and on critical vulnerabilities for NATO future missions.*

National Reserve Forces Committee

After its NATO accession, Romania was invited, in February 2005, to become a fully fledged member of the *National Reserve Forces Committee – NRFC* and to participate in the activities conducted by it. *NRFC is the Alliance central forum* responsible for reserve matters and it serves as a committee to provide policy advice on reserve issues to NATO's Military Committee as well as to assist and provide advice to the *Interallied Confederation of Reserve Officers – CIOR*³ in the activities performed by it in order to meet the Alliance goals.

NRFC was established in 1981 as a forum for NATO as well as CIOR member nations to exchange information regarding reserve matters. NRFC was accredited by NATO Military Committee in November 1996 and performs its activity based on the following documents: *NATO Military Committee Directive no. MC 392/1998 regarding the relation between NRFC and NATO; NATO Military Committee Directive no. MC 248-1/1998 regarding the relation between CIOR and NATO; NATO Military Committee Directive no. MC 317-1/2002 regarding NATO force structure; NATO Military Committee Directive no. MC 441/1 regarding NATO policies on Reserve Forces; Memorandum of Understanding between CIOR and NRFC in February 1998, updated and completed in 2003.*

*The main objectives of NRFC are: to strengthen the Alliance reserve readiness by providing an open forum for the exchange of information and lessons learned; to provide NATO Military Committee with advice on reserve matters; to support CIOR in the activities it performs to the Alliance benefit*⁴.

³ Interallied Confederation of Reserve Officers is commonly referred to by its French acronym CIOR.

⁴ Cf. MC 392, *Relationship between NRFC and NATO*, approved by the MC, NATO HQ, 27 March 98.

Currently, following Croatia joining the committee, there are 24 NRFC member states. Australia is a permanent observer. In the future, Austria, Finland, FYR of Macedonia⁵, Sweden and Switzerland can also join NRFC. Moreover, there is a representative from ACT, ACO and IMS. Its composition, in principle, is presented in *figure 1*.

NATO has begun the process of reviewing the MC documents governing the reserve forces in order to harmonise them with the new Strategic Concept requirements and to share the best practices regarding the reserve forces organisation, establishment, use and maintenance in the future, in the context of restructuring the armed forces in many member states⁶. The process of reviewing these documents is managed by the IMS, supported by NRFC and CIOR. Country delegations are made up by officers with responsibilities for the reserve forces mobilisation, having the mandate to express views on the issues under discussion. Each member state provides a delegation of 2-4 members (a head of delegation and 1-3 staff officers).

NRFC Chairmanship is held by an officer having the rank of general from one of NATO member states, for a period of 2 years. The Chairman's mission is to organise and conduct the committee meetings, as well as to coordinate its activity. Currently, the Committee's Chairmanship is held by France.

NRFC meets twice a year, in winter, usually at NATO Headquarters in Brussels, and in summer, in different member countries, usually at the same time with the CIOR meeting. These activities are planned and prepared by staff officers meetings, in spring and autumn, between the Committee working sessions.

So far, in the meetings attended by the Romanian delegation, the activities have been conducted under the motto *transformation – integration – motivation*. Most NATO member states have reorganised their armed forces, reserve forces included, to be better prepared for future missions. This fact has had a significant effect on the structure of reserve forces too.

To reflect the growing importance of reserve forces in NATO-led operations, during NRFC activities, the focus has been on presenting some topics related to the training of reservists to participate in NATO operations, joint or multinational ones. This aspect was emphasised by the chairman of the NATO Military Committee, General Raymond Henault, as well as by the commander of NATO Response Force in Brunssum/the Netherlands, General Back, who indicated that professional training and experience were important elements that allowed reservists to have training equivalent to that of active forces and, therefore, as many reservists as possible have to be trained at the level of active forces.

⁵Turkey recognises the Republic of Macedonia with its constitutional name.

⁶Cf. *NRFC and CIOR annual reports*, presented during the Military Committee in Permanent Session, NATO HQ, Brussels, 7 July 2011.



Figure 1: NRFC and CIOR Composition⁷

⁷ See http://www.cior.net/getattachment/About-CIOR/Key-Documents/Dutch_Presidency_Booklet.pdf.aspx

Regarding *reserve forces training to participate in international missions*, NRFC contacted NATO Defence College in Rome and NATO School in Oberammergau to expand reservists' opportunities to train in NATO institutions. As a result, NATO Defence College has established modular training courses for reserve officers and at NATO School in Oberammergau several series of reserve officers in different NRFC member countries have already participated in training courses⁸.

Furthermore, based on cost implications and educational constraints, it is studied the possibility for reserve officers to use the distance learning methods (e-learning) provided by NATO Defence College or ACT. The necessary themes and information can be accessed on ACT website, reservists having the possibility to choose the modules and topics they want to study, each module being completed with an assessment test, depending on the available time.

The advantages of this method are represented by the minimal cost compared to the cost of academic training, the increased access to a wide variety of topics, as well as by the fact that new concepts and domains are made easy to understand by reservists. However, there are also *disadvantages* such as the fact that reservists have no access to special topics, there is no direct discussion with teachers, and the interaction with other students is low.

The goal of NRFC educational campaign is to improve the knowledge and understanding of NATO values, political-military concepts, their external-internal adaptation, new missions, potential security risks, NATO member countries political, security, defence and socioeconomic systems, the major role of international organisations in the Euro-Atlantic security, business trends that may influence NATO security. Briefly, reserve officers must have an equal qualification to that of active officers, when they temporarily serve in NATO-led operations worldwide as well as in NATO headquarters.

As a recurrent problem within NRFC meetings, aspects related to the support provided by the member nations engaged in developing new force structures to respond to the roles assumed by NATO have been debated. Many nations have initiated measures meant to change the model of the force structure having subunits, units and large units based on conscription to the force structure based on professionalism and volunteerism. Any change in the structure of the active forces will eventually have an impact on the structure of reserve forces. NRFC provides examples of reserve structure models through which the engagement of reserve forces to support internal and international operations can be facilitated. Moreover, NRFC discusses regularly about adopting best practices as far as the relationship

⁸ Cf. *NRFC Committee Report*, NRFC Summer Congress, Stavanger, Norway, 2010.

between the reserve structure and specific policies is concerned, to support the concept of operational reserve.

Starting 2010, NRFC has focused its activities and discussions on operational issues, especially those related to the reserve support provided to NATO operations, using the framework of the current operations in Afghanistan. The discussions have covered the full range of reserve forces capabilities (from niche capabilities such as Civil-Military Cooperation – CIMIC, which benefit from the professional qualifications of reservists, to highly qualified capabilities, which may be generated by a focused and well managed reserve training programme).

Another highlighted aspect is that regarding the *employers support* in relation to reserve forces. In countries such as Australia, Canada, the UK, the USA, special structures are established within the ministries of defence, which are in charge of solving the problems regarding the reservists support in the relation to their employers. There is specific legislation establishing the rights and responsibilities of employers and employees that are part of the reserve component and participate in missions with the armed forces.

At national level, NATO member states reassess the support provided to different *reservists' associative structures*, mainly as a result of ongoing budget cuts. National reserve forces organisations/federations are composed of a wide range of retired military personnel as well as a significant number of volunteers. More precisely, there are two types of members in these organisations: *active reservists*, performing national missions or international missions for active military personnel (former active military personnel, former conscripts etc.) and *non-active reservists*, who are attached to these organisations and are given special attention as, in most cases, they are senior (influential) people in the civil society, local public authorities or even members of the parliament⁹.

In the following years NRFC preoccupations will focus on:

- continuing to support NATO transformation by working with ACT and conducting meetings at the ACT headquarters where there is the possibility to disseminate information and share experience;
- reserve forces are a national responsibility and, therefore, each country may have structures, roles and policies that are specific to national requirements and international commitments;
- enhancing motivation to recruit and attract reservists in the armed forces, considering that more and more countries give up conscription;

⁹ France, for instance, has two deputies and two senators whose responsibilities are oriented towards reservists matters.

- as a recognition of the important role played by reserve forces in support of current operations, NRFC will continue to act to ensure an appropriate professional development, as part of training, including through the participation of reservists in NATO-led collective exercises;
- continuing the participation of reserve officers in the training provided by Joint Forces Staff College, the USA, as well as in the exercises conducted by ACT.

The cooperation between NRFC and ACT is established based on mutual agreements, according to each area of responsibility, both bodies having the common mission and interest in NATO transformation, and recognising each other as transformation agents, ACT being “NATO’s leading agent for change, driving, facilitating, and advocating continuous improvement of Alliance capabilities to maintain and enhance the military relevance and effectiveness of the Alliance”¹⁰.

In this respect, NRFC agrees to promote the transformation programme through communication with MC, CIOR and nations, to actively involve in ACT missions to support national reserves through exercises, expertise, and other operations, to maintain information integrity within NRFC by using ACT web pages. Moreover, ACT agrees to host NRFC periodical meetings at the ACT or ACT subordinate headquarters in Europe, to support NRFC initiatives for the reserve component courses in NATO educational institutions and to host the Reserve Wise page on the ACT website.

Interallied Confederation of Reserve Officers

“The 800 000 reserve officers in CIOR represent an invaluable and indispensable support for the Alliance. I have no doubt that the new NATO strategy will predict a higher dependence on the Reserve Forces to further provide effective defence and deterrence”¹¹.

The Interallied Confederation of Reserve Officers is a non-political, non-governmental and non-profit organisation meant for cooperation between the national associations of reserve officers. The numerous contacts and visits between the national associations of reserve officers from Belgium, France and the Netherlands took place from 1935 to the moment the Second World War broke out, and resumed from 1946 and November 1948, culminated with the organisation of the first congress in Brussels, Belgium, when CIOR was officially established, event that was attended by observers from the national associations in Canada, Luxemburg, the UK and the USA.

¹⁰ Cf. <http://www.act.nato.int/general-info/history-of-allied-command-transformation>

¹¹ NATO Secretary General, opening speech, CIOR Summer Meeting, Calgary, Canada, 2008.

Subsequent to CIOR establishment, other reserve officers associations in NATO member countries have joined it, starting with Luxemburg in 1952, followed by Denmark in 1956, Greece in 1957, the USA in 1958, Italy in 1961, the UK in 1963, Canada in 1964 and Norway in 1966. Currently, CIOR covers an area between the Mediterranean Sea and the Pacific Ocean and guarantees the defence-related interests of over 600 million of people. In CIOR records, there are reserve officers, members of national organisations, working in industry, education, business, academic and political environment, many of them holding leading positions in these fields of activity, being thus able to provide relevant information related to defence issues.

In accordance with the statute and legal rules of operation, the CIOR *main objectives* are: to contribute to strengthening deterrence and defence capabilities of NATO and signatory states; to support NATO policies and to contribute to the achievement of objectives by the Alliance; to stay in close contact with all NATO authorities and military commands; to establish and develop contacts between reserve officers to enhance mutual knowledge and understanding; to stay, through national associations, in close contact with defence bodies; to achieve uniformity as far as the obligations, rights, training and mobilisation of reserve officers within NATO are concerned, while respecting national differences and traditions.

The relationship between CIOR and NATO, which has been intense over years, was formalised in 1976 when the supreme NATO military authority, the Military Committee, approved the document MC 248, which regulated military cooperation between NATO and CIOR. Subsequently, a permanent CIOR representative was appointed to the International Military Staff. At the political level, the liaison officer for defence intelligence within NATO Intelligence Department has, on behalf of the Secretary General, the responsibility for not only the official contact between NATO and CIOR but also for providing advice on political issues. Based on a recommendation in MC 248, an advisor on the Reserve Forces issues was appointed to the Supreme Headquarters Allied Powers Europe – SHAPE.

NATO and SHAPE support educational and informative activities for reserve officers. All 20 courses organised at NATO/SHAPE School in Oberammergau are open to reserve officers. Every two years, NATO Defence College in Rome organises a one-week course for reserve officers in NATO countries.

Annually, a seminar is held at NATO and SHAPE to keep the young reserve officers informed. In addition, during the CIOR congress, a workshop for young reserve officers is organised. Every two years, NATO and SHAPE host a seminar for experienced reserve officers and, in alternative years, another seminar for the editors of the journals of reserve officers. It is obvious that after the CIOR

Congress in Strasbourg, in 1952, which decided the establishment of permanent relations with NATO, much has been achieved related to the CIOR enhanced contribution to defence.

In order to achieve its objectives, CIOR meets every year, each time in a different member country. Congresses, which last for five days, are held in July or August. On this occasion, current issues related to NATO and its reserve forces are discussed. In addition, there is communication and interaction between NATO reserve officers. During the congress, a military competition is conducted, consisting in military orientation, individual firing sessions, obstacle course, swimming and first aid. As it has already been mentioned, simultaneously with the summer congress, a *workshop* for young reserve officers is organised. The host national organisation is exclusively responsible for the detailed planning and organisation of the particular congress.

The Executive Committee and Commissions winter meeting is held at NATO Headquarters in Brussels, Belgium, usually in the first week of February. During the meeting, the issues are continued to be discussed, the activities of the summer congress are completed, in cooperation with the International Military Staff.

The national associations of reserve officers represent the CIOR core. However, they remain completely independent as far as national issues are concerned. CIOR delegates are elected among own members, and the chief of each delegation becomes one of CIOR vice chairmen. The Chairman and Secretary General are elected for two years and are part of the same national association.

The Executive Committee, the supreme CIOR authority, is composed of the Chairman, Secretary General, Vice Chairman and more four delegates on behalf of each national association. The Executive Committee is the body responsible for the policy and decides which country will assume CIOR chairmanship, where the meetings will be held, which the projects assigned to different commissions are and what actions will be performed to complete these projects. The CIOR financial body records the annual contributions of the member national associations. These funds are supplemented by donations, grants and bequests.

On behalf of the Executive Committee, six standing commissions having specific attributions are operational. Each national delegation is represented by at least one member for each commission. All commissions have a chairperson, a vice chairperson and a secretary, positions held for two years with the possibility of re-election for more years. The responsibilities of commissions are the following: *Commission 1* (Reserve officer status, mobilisation, education, training and data exchange) examines and suggests ways of improving NATO defence by the use of member reserve forces; *Commission 2* (Defence issues and attitudes) exchanges

information related to member nations attitudes, events and trends affecting NATO, studies disinformation related to NATO and its reserves; *Commission 3* (Public relations and information) exchanges information on public awareness of NATO, its defence and its reserves, recommends press and information policy and helps to promote NATO in member countries, supports the Executive Committee in general policy and planning areas; *Commission 4* (Legal affairs) studies legal matters affecting NATO, its defence, and its reserves; *Commission 5* (Civil defence and emergency planning) exchanges information on disaster preparation and emergency procedures in member nations, including command and control, preparation, planning and training; *Commission 6* (Military competitions) directs and monitors the conduct of the CIOR military competitions.

BIBLIOGRAPHY

1. ***, ACT DIR 45-2, *Responsibilities for the Management of US Reserve Component (RC) Personnel in Allied Command Transformation (ACT)*, HQ SACT, Norfolk, Virginia, 2006.
2. ***, AJP-9, *NATO CIMIC Doctrine*, NATO HQ, Brussels, 2005.
3. ***, AJP-01 (D) *Allied Joint Doctrine*, NATO HQ, Brussels, 2010.
4. ***, J.P. 4-05.1, *Joint Tactics, Techniques, and Procedures for Manpower Mobilization and Demobilization Operations: Reserve Component (RC) Callup*, NATO HQ, Brussels, 1998.
5. ***, MC 248-1, *Military Committee Directive*, NATO HQ, Brussels, 1998.
6. ***, MC 392 (Revised), *MC Directive for Recognition of the National Reserve Forces Committee (NRFC)*, NATO HQ, Brussels, 1998.
7. ***, MC 317-1, *Military Committee Directive*, NATO HQ, Brussels, 2002.
8. ***, MC 0519, *NATO Military Committee Concept regarding Reserve Forces*, NATO HQ, Brussels, 2005.
9. ***, MC 441/1, *Military Committee Directive*, NATO HQ, Brussels, 2005.
10. ***, MCM 0007, *NATO Military Committee Decision regarding the relation between NATO Response Force and Reserve Forces*, NATO HQ, Brussels, 2005.
11. <http://transnet.act.nato.int>, <http://jadr.act.nato.int>

English version by
✍️ *Diana Cristiana LUPU*

DEMANDS ON NATIONAL OPERATIONAL COMMUNICATIONS SYSTEMS FOR THEIR INTEGRATION INTO UNIFIED COMMUNICATIONS SYSTEMS IN COALITION OPERATIONS

Colonel Daniel BRĂTULESCU

The author discusses the importance of integrating national operational communications into the Unified Communications Systems currently used in the theatres of operations.

In this respect, the trends and necessary courses of action to ensure timely and effective information transfer and the UCS interoperability, the standard models considered essential in the design and implementation of operational information transfer, the vulnerabilities and threats to the UCS security are mentioned.

In conclusion, it is shown that the need to identify and address the demands on national operational communications systems for their integration into UCS is the current concern of those in charge.

Keywords: *standardisation; interoperability; communications and information systems; encryption*



The integration of national operational communications into Unified Communications Systems (UCS),

used in current coalition operations, enables the traditional communications and information systems transfer to these systems as well as the planning and organisation of secure communications and information services, defined by the unified communications platform system architecture as a full range of technological solutions, coherent information management capabilities, interfacing applications and technical compatibility, priorities and/or restrictions on users access to packages of data circulating, and coherent management of the entire stream configured in the coalition military action.

The UCS interoperability supplements the means to transfer information to the forces participating in the operation and diversifies communications and information services provided to users, according to information exchange requirements by interconnecting, within the specific

Colonel Daniel Brătulescu – the General Staff, the Ministry of National Defence.

architecture, the equipment and means of communications belonging to traditional communications and information systems, organised in compliance with the security and interfacing conditions accepted by the coalition, and with the operational requirements of the mission command and control.

Unified Communications Systems • Interoperability • Measurable objectives • Information assurance

The demands on national operational communications systems for their integration into unified communications systems in coalition operations are represented and defined by the ways the unified communications systems interoperability requirements are assimilated.

This fact generates the need to identify and implement, over the course of coalition military operations, measures and actions considered appropriate by experts in the field to address specific aspects of technical compatibility and procedural systems in operation, to ensure a timely and efficient information transfer, able to meet the command and control operational requirements throughout the mission.

The guidelines and principles for achieving UCS interoperability in current coalition operations conducted in Afghanistan are represented by the following trends and necessary courses of action to ensure timely and effective information transfer:

- *continuous interoperability*, representing a constant concern for increasing technical compatibility and interconnection possibilities;
- *centralised responsibility*, meaning that the Joint Task Force Headquarters (JTF HQ) assesses the level of interoperability of the connected systems and networks in the entire theatre of operations;
- *communications and information architecture based on services*, defined as a system facility to use integration platforms and interfacing capabilities to consistently provide communications and information services;
- *unified management of access and interconnection points*, represented by the possibilities to control the access to classified networks and to certify/accredit, according to the standards accepted in the coalition, the users rights to access confidential information in the theatre of operations;
- *adaptability*, defined by efficiently running the activities and technical procedures to technically reconfigure the systems, in order to ensure appropriate services, able to meet the mission operational needs;
- *measurable objectives* related to interoperability, based on procedures, standards and protocols that are consistent, timely and efficient, adapted to tasks and that, due to the compatibility, architectural integration

and convergence of the component systems, ensure the traditional communications and information systems transfer to UCS;

- *technical certification and accreditation*, represented by the specific requirements communications and information equipment and means should meet, in compliance with the coalition standards, related to interconnection in the open technical architecture installed in the theatres of operations.

The basic organisational principles underlying the proper conduct of the UCS information assurance process, during coalition military actions, which define and represent the way of planning, organising and implementing communications and information during the course of Operation “*Enduring Freedom*” and can be considered demands on national operational communications systems for their integration in the UCS are as follows:

a) *Communications and information services used by users are our services, and their mission is our mission*. The principle demonstrates how seriously the communications and information capabilities available to coalition forces participating in the mission are planned, organised and implemented, highlighting the need for specific equipment and resources to meet the requirements and standards for unified communications interoperability and compatibility, as well as for their reliability and technological consistency. In addition, collaborative measures between IT experts participating in the mission are needed to meet all user requirements and to identify, in support of own forces and coalition partners, in due time, the technical solutions considered optimal. The principle identifies and demonstrates the high level of confidence in ensuring the success of the operation, by assigning a key role to UCS services, available to all users participating in the mission.

b) *Information transfer performed by UCS reflects the specific information assurance needs as required by the operation command and control*. The UCS architectural infrastructure and terminals/voice, data, and VTC equipment are planned, organised and distributed to the forces participating in coalition military operations in order to define and meet the mission information assurance needs and requirements, which generates the opportunity for the information transfer to meet operational command and control needs.

c) *Security threats to the UCS communications and information systems must be anticipated and countered by specific actions*. The principle emphasises that the UCS communications and information services vulnerabilities should be anticipated and presented to the personnel responsible for organising the equipment and technical means that are part of the unified communications system and architecture

who, by identifying standards, specific hardware and software applications, can monitor the effective operation of the system, eliminate or reduce the effects of possible threats and, also, by their own research and technological development efforts, enable the anticipation of possible sensitive security areas/issues. A key role in this respect is played by not only the compliance with security measures and policies agreed at the coalition level but also by the implementation of networks encryption and classification procedures, which define the information transfers planned, organised and performed by UCS.

d) *Contemporary information society developments trigger the continuous evolution of communications and information services configured by UCS, providing information supremacy.* The idea defines the need for current technology developments to be rapidly assimilated and adapted to the specific systems used in coalition operations, to develop and modernise the services provided to participants in the mission, in order to identify some information transfer additional capabilities¹.

The principle defines and characterises the UCS infrastructure as a system architecture that has to meet the technical requirements of adaptability and flexibility, of reconfiguration to the needs of command and control, and to provide the circulation of confidential information securely, in order to ensure own forces information supremacy.

e) *Communications and information resources allocated and specialists' readiness generate the level of ambition.* The logistic possibilities of the forces participating in international missions in theatres of operations, the assimilation of new technologies specific to the communications and information systems, and the education and training of specialists are basic conditions in the organisation and provision of specific, timely and effective services, which may significantly influence the success of the assigned missions, by meeting performance standards, as well as technical and procedural interoperability and compatibility requirements.

The measures meant for the unified communications systems information assurance consist of specific activities related to planning, organisation, verification, availability, coordination and supervision of diversified communications and information services provided, encrypted and clear, according to coalition operations information exchange requirements (IER) that meet the security standards agreed in the theatre of operations.

These measures are represented, in the UCS component communications and information centres, by protocols and software applications that, besides ensuring unified communications capabilities, are aimed at implementing and verifying the way in which the secure information transfer is organised and performed.

¹ Dennis Hartmann, *Chapter 1: Cisco Unified Communications Manager Architecture*, Network World, USA, 25 July 2008, pp. 3-11.

The possibilities to achieve secure unified communications², under the conditions of coalition military operations, are represented by the opportunities to ensure, depending on the operational command and control needs, communications and information services, timely and efficient, which meet the specific requirements related to the security, confidentiality, and integrity of data and information transferred between users. The capability thus defined and generated by the UCS is the omni-directional transfer and replication of voice, data, and video teleconferencing (VTC) signal, depending on the specific operational requirements and the distribution and representation possibilities of the services available in the area of operation of the installed architectural infrastructure.

The ways to provide solutions, in a timely manner, to the information needs generated by the command and control requirements specific to coalition operations are anticipated, planned and organised by the UCS through the multiple opportunities provided by the system for the transfer, in real-time, of communication and information services throughout the operational control hierarchy. The high information flow transport capacity, supplemented by systemic technical facilities that meet the security standards and are represented by specific interface procedures and applications, which provide a high degree of interoperability and architectural compatibility, leads to the characterisation of the UCS as a system able to provide users with diverse and multiple secure communications and information services³.

Demands on national operational communications systems for their integration into unified communications systems in coalition operations

The possibilities to transfer and integrate national operational communications systems into the UCS can be quantified by specific actions meant to measure and represent the level of interoperability of the UCS used in current coalition operations, in which the following *standard models*⁴, considered essential in the design and implementation of operational information transfer, are identified and configured by analysing the system degree of acceptance:

- Spectrum of Interoperability Model (SoIM);

² *Unified Communications Security: A Best-in-class Strategy to Unleash Value*, Aberdeen Group 2011, <http://www.redscan.com/sites/default/files/documents/Aberdeen-Group-UCSecurity-Feb2011.pdf>, retrieved on 22.02.2013

³ *Cisco Unified Communications System Release 9.x SRND*, Americas Headquarters Cisco Systems, San Jose, USA, 28 June 2012, pp. 2-4.

⁴ Jo Ann Lane & Ricardo Valerdi, *System Interoperability Influence on System of Systems Engineering Effort*, University of Southern California & University of Arizona, SoSE Collaborators Information Exchange, USA, 2012, pp. 3-8.

- Levels of Conceptual Interoperability Model (LCIM);
- Quantification of Interoperability Methodology (QoIM);
- Layers of Coalition Interoperability (LCI);
- Military Communications and Information Systems Interoperability (MCISI);
- NATO C3 Technical Architecture Reference Model for Interoperability (NMI);
- Levels of Information System Interoperability (LISI);
- System-of-Systems Interoperability Model (SoSI);
- Interoperability Assessment Methodology (IAM);
- Organisational Interoperability Agility Model (OIAM);
- Organisational Interoperability Maturity Model for C2 (OIM).

The criteria and courses of action related to the UCS used in current coalition operations interoperability are designed to prepare and guide the activity of testing the equipment, tools, and hardware and software applications composing the systems to achieve the proposed interconnection level. They are as follows:

- procedural and technical interoperability strategy regarding communications and information systems used in coalition military operations is established at the JTF HQ, in accordance with the operational control requirements specific to the theatre;
- responsibility for planning, organising and performing information transfer from the theatre of operations to the large units of brigade type (similar) lies with the JTF HQ;
- the UCS architectural infrastructure installed in the operational environment will allow the connectivity of the communications and information systems that equip coalition forces, in compliance with NATO technical and procedural compatibility standards;
- communications and information centres installed in the theatre of operation will allow the implementation of interoperability standards and procedures agreed by NATO, complemented with those mentioned in Appendices Q (Communications and IT) at the coalition level;
- the way the communications and information system is planned and organised will seek to maximise systemic networking;
- voice, data and VTC services, encrypted and unencrypted, organised in the operational environment, will be transferred hierarchically, in compliance with interoperability standards and the security policies agreed by the coalition;

- the information transfer will be performed according to the UCS information exchange requirements, through sharing the interoperable channels organised in the theatre of operations.

The interoperability challenges⁵ related to the services provided by the UCS used in current coalition operations as well as to the transfer of the traditional communications and information systems to the UCS are as follows:

- the representation and configuration of communications and information services transferred between systems should be organised in a standardised manner, using IP conversion of the signal, employing “*Everything over IP*” (EoIP) strategy;
- the distribution and allocation of services to users should be achieved dynamically, observing the network classification levels, the standards and protocols accepted by the coalition, and the mission operational requirements, in conformity with command and control needs;
- planning and providing theatre level communications and information services should be defined in relation to the mission information exchange requirements, the systemic interconnection criteria agreed by the coalition forces, and the specific compliance and interfacing requirements, represented by the technical characteristics of component elements and the implementation/acceptance of interoperability standards;
- the standardised identification and definition of the system gateways and entry points should be performed according to the interoperability requirements and security policies agreed by the coalition.

The integration of communications and information services provided in Afghanistan, during the coalition operations, is currently represented by activities meant to consolidate the existing technical infrastructure, and to increase the technological efficiency and mobility of the installed centres, in order to supplement the possibilities to assure the operational information transfer. These trends lead to creating a technical and procedural interoperability environment, being focused on setting up a unified architectural infrastructure that is defined by the following characteristics:

- integrated approach to the communications and information services available to users to meet information assurance (IA) requirements;

⁵ Frank T. Johnsen, Marianne Rustad, Trude Hafsoe, Anders Eggen, Tommy Gagnes, *Semantic Service Discovery for Interoperability in Tactical Military Networks*, The International C2 Journal, CCRP, USA, Vol. 4, No. 1, 2010, pp 2-6.

- implementation of new field-specific capabilities and technologies (unified communications, cyber insurance, cloud computing);
- coherent consolidation and rationalisation of communications and information services provided to meet the command and control requirements, according to the security policies agreed by the coalition.

The responsibility to ensure consistent and effective exchange of information leads to the need for proper application and development of interoperability standards regarding the content, quality and integrity of data and information conveyed by communications and information services, in which case the implementation of interoperability procedures generates the following key benefits to the system design:

- ⇒ reduced period of assimilating the new technologies generated by the evolution of contemporary high-tech society;
- ⇒ reduced costs of equipment and communications and information means development and integration, as well as of those related to the UCS components lifecycle;
- ⇒ improved networking capabilities and technical compatibility, which generates supplementary opportunities to achieve the systems interoperability.

We appreciate the need for consistent performance of specific procedures to minimise/limit the effects of threats to the UCS security as a demand on national operational communications systems for their integration in the UCS used in coalition operations. These threats are identified as a result of planning, organising and performing information transfers, in international environment, between the users participating in coalition operations, represented and defined by *identity theft* or *creating/generating an ambiguous identity*, and characterised as the most commonly used attacks to steal confidential information by an unauthorised person. In order to obtain confidential information, hackers can use an application called *Trojan horse*, which enables the user identification and password transmission, or a *network sniffer* that, in case of unencrypted messages and data transmissions, can “*smell*” the network architecture and inspect/capture the computer traffic to be relayed to an unauthorised user. To protect the UCS against these security threats, we consider necessary to implement specific procedures for recording and archiving system transfers so that they could be subsequently analysed and, by using content filtering applications, any file that contains viruses or other software applications, used by opponents for information leaks, could be identified.

A specific UCS vulnerability coming from the cyber environment⁶ is represented by the security risks the system exchange server is subject to, risks characterised as technological derivatives of denial of service, leading to unauthorised exposure of own confidential information. Denial of service by the system server can be achieved through *virus* or *malware*-type applications by flooding the voice, data, and VTC networks with false requests, which generates increased traffic and leads to the impossibility of the system to process all orders. In addition, we mention the vulnerability specific to IP converted signal, characterised by the ability of an external user to intercept and identify transferred IP products, using an IP data package analyser, and later, after learning the identification data (ID), to discover and recognise the information transferred. The effects of this action can generate significant security incidents, with essential consequences for the coalition operations command and control, since the hacker is able to redirect communications and information services, reconfigure the system IP addresses, and/or transmit inaccurate data. The loss of identity can be eliminated by encrypting the signal and information flows transferred between users, by using gates that can withstand the signalled attacks, and by implementing advanced software to monitor and encrypt traffic as well as to detect anomalies related to the UCS standards/protocols.

We consider that encryption of voice, data and VTC services in the UCS used in coalition operations can be achieved by implementing and using two specific keys for encryption: *call signalling encryption* (exchange server and used terminal) and *stream encryption* (information transfer between communications and information centres). We present, as shown in *figure 1*, the encryption of voice services in the UCS.

To sustain the efficiency and IP availability of the devices connected in the UCS, we suggest taking into account, by specific software applications, the degree of fault tolerance for the useful signal, and identifying and addressing specific aspects of redundancy to eliminate any accidental failure occurring in the system operation.

The need to identify and address the demands on national operational communications systems for their integration into unified communications systems in coalition operations is the current concern of the exponents of communications

⁶ Eileen Kowalski, Dawn Cappelli, Andrew Moore, *Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector*, National Threat Assessment Center United States Secret Service & CERT®Program Software Engineering Institute Carnegie Mellon, Washington DC & University Pittsburgh, 2008, pp. 15-29.

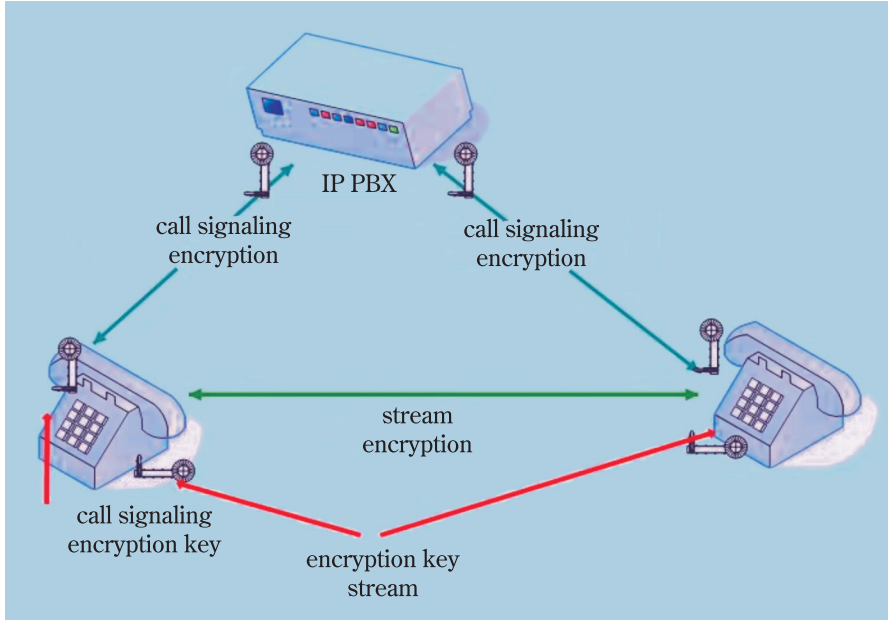


Figure 1: Encryption of voice services in the UCS used in coalition operations

and information systems. In this respect, running the UCS interoperability process, in compliance with specific standards and procedures, is a current requirement related to the implementation of these systems in the coalition operational environment, which is generated by the continuous development of equipment and communications and information means and by the need to integrate them, in a timely manner, into the system architecture installed in the theatres of operations in order to ensure an effective information transfer within communications and information services, defined and adapted to the mission command and control requirements and needs.



INFORMATION WARFARE BETWEEN THREAT AND FORCE MULTIPLIER

Fleet Rear Admiral (N) Dr Cătălin-Silviu DUMISTRĂCEL

The development of information infrastructure, which includes media structures, can generate increasingly sophisticated communication opportunities. Thus information can be conveyed at a more accelerated pace and at a larger distance. To this end, according to the author, an essential condition is that all these information conglomerates should not be controlled by certain decision centres that can try to limit people's access to information resources. For decades, the USA has cultivated the best and most intelligent devices in the field of communications and control, in accordance with the new technological advancements.

Keywords: *nuclear weapons; information systems; state of security; Romanian espionage*

Concepts, Theories, Definitions

The concept of *security* means a situation in which a person, group of persons, state, alliances, following specific measures adopted individually or through an understanding with other actors, feel certain that their existence, integrity and fundamental interests are not jeopardised. If the term *security* means peacefulness, the feeling of being out of danger, of being protected, *insecurity* is opposite to security and involves anxiety, a feeling of danger and risk, of being threatened, limited freedom.

Security is achieved at all levels of social organisation (individual, group, state, alliances) and is manifested in all areas of existence: political, economic, social, military, demographic, ecological, cultural etc.

Security is generated by the political factor and must cumulatively meet the following conditions:

- it must be a state action, carried out based on a normative system;
- it must be a matter of state institutions;
- political power must be legitimate and the rule of law must prevail;

Fleet Rear Admiral (N) Dr Cătălin-Silviu Dumistrăcel – Deputy Chief of the Structures and Acquisition Planning Directorate, the General Staff, the Ministry of National Defence.

- the actions must be based on a system of values accepted by society;
- the respect for human rights must be in accordance with international regulations to which the state is party;
- it must not cause insecurity to other entities¹.

In the category specific to security, one may mention terms such as: risk, threat, danger, security status, aggression, conflict, national interests, vulnerability, security objectives, security system, security environment etc.

To enhance the security of an actor (state, organisation, coalition etc.) and to generate insecurity for an adversary or potential adversary, “information” management is of paramount importance, namely: captured information versus lost information, “powerful” information, of great effect, versus “weak”, uninteresting information, protected information versus disclosed information etc., these representing the ammunition used in “combat”, what we now call *information warfare*. The most appropriate verbs to describe these elements are: *to co-opt, to send, to quickly process information, to prevent the opponent from doing the same, to distort, to misinform or to protect own infrastructure*.

Information warfare is a domain to be defined, but which is given increasing attention and resources, given the rapid progress of information technology in the past decades. In *information warfare*, information is *resource, target and weapon* at the same time.

Among the first to attempt to define the term *information warfare*, one may include Alvin Toffler, who, in his work, *The Third Wave*, published in the US in 1980, said that “one way to attack a nation is to restrain the flow of information – cutting off contact between the headquarters and overseas branches of a multinational firm, building information walls around a nation etc.”².

The approach to the concept of *information warfare* is very different and its ambiguity increases as expressions such as: *cyber warfare, network warfare, third wave warfare, post-industrial era warfare* are used.

The different forms of *information warfare* have many elements in common in terms of objectives, means and methods used, instruments with which the goal is pursued. This brings to mind the *activity of espionage* as an instrument of *information warfare*, which has been a fearsome weapon throughout history and continues to pose a major threat to global security.

¹ Dănuț-Mircea Chiriac, *Politici și strategii de securitate la începutul secolului XXI*, Editura Universității Naționale de Apărare “Carol I”, București, 2005, p. 5.

² Gelu Alexandrescu, Ion Călin, Costinel Nițu (coord.), *Securitate și apărare în Uniunea Europeană, Strategii XXI/2008*, 17-18 aprilie 2008, Secțiunea 7 – Sisteme informaționale, Editura Universității Naționale de Apărare “Carol I”, București, 2008, p. 46.

In general, *information warfare* includes those actions carried out against the enemy or potential enemy's intelligence or information systems, while protecting own intelligence and information systems, with the purpose of reaching certain goals or influencing certain enemy targets. There are three aspects of *information warfare* that must be considered:

- to obtain and consistently and rigorously fill in information about the enemy
 - information collection;
- to prevent the opponent from obtaining new real pieces of information
 - information protection;
- to launch inaccurate information or deliver it directly – misinformation.

There is nothing in this world better rooted in the practice of nations, epochs and civilisations than espionage. After prostitution, espionage is the world's oldest profession. The Bible itself presents a situation where God tells Moses: "*Send some men to explore the land of Canaan, which I am giving to the Israelites. From each ancestral tribe send one of its leaders*". They were the first Biblical spies, to whom the Creator gave the mission to go and "*see what the land is like and whether the people who live there are strong or weak, few or many*".

The simplest definition of espionage is that it is an activity carried out by specially trained personnel in order to follow people, institutions, organisations and countries to learn their intentions, capabilities of any nature, habits, actions etc. and to inform a third party.

The term *espionage* is often associated with the state that spies on its potential or actual enemies, primarily for military purposes. Consequently, the term has been extended to all domains of social life where obtaining data or information is done without the consent of the holder (owner), illegally, being thus outlined other forms of espionage: economic, cultural, financial, IT etc. Many nations spy, at a given time, both enemies and allies, while maintaining a policy of not commenting on this.

The Influences of Information Warfare on Global Security

The development of information infrastructure, in full process of globalisation, which includes media structures, generates increasingly sophisticated communication possibilities. Information is sent at a more and more accelerated pace and increasing distances. The essential prerequisite for this to happen is that these information conglomerates are not controlled by certain decision-making centres that can try to limit people's access to information resources.

Information attacks are not new. For decades, the United States of America has grown the best and most intelligent communications and control devices,

in accordance with the new technological advancements. The means and methods of espionage advanced concomitantly, the surveillance and data transmission being done in real time, with high precision electronic equipment. The “Cold War” caused intense espionage actions on the part of both military blocs – the US and its allies, on the one hand, the Soviet Union, China and their allies on the other hand – which focused mainly on the nuclear issue. At one point, there was even mentioned the superiority of the Soviets in that area. With the collapse of the Soviet bloc, part of the intelligence agencies became specialised in missions for the detection or tracking of terrorist networks, drugs, weapons traffickers, organised crime networks, “cyber pirates” etc.

The novelty in the field stems from the use of scientific research results for designing messages so that they have the desired effect, as well as the use of modern channels for sending them, which enhances the possibilities of information aggression. Information confrontation consists in targeting the pieces of information and information functions of the enemy, while protecting own ones, with the intention of defeating its will, either it is state, institution or individual.

Strictly militarily, *information warfare* consists in all information operations carried out at tactical, operational and strategic level, in peacetime, during crisis and at war in order to gain supremacy.

In NATO’s vision, the military component of *information warfare* – command and control warfare – requires the integrated use of all military capabilities, including security operations, supported by all sources of “*intelligence*” and communications and information systems, in order to influence, damage or destroy an enemy’s command-control capacity, while own capabilities are protected against similar actions. During conflict situations, in the new circumstances, opponents will have simultaneous access to huge amounts of information, but the one to have the most accurate and complete ones and benefit from an efficient system for processing and protecting them will be at an advantage.

However, the term *information warfare* is not used only in the military domain, being taken and adapted in almost all economic and social domains. Thus, we can discuss of *corporate information warfare*, which describes the competition or, rather, the continuous “*espionage*” between private companies through stealing, destroying, researching results, disseminating false information in order to sell products etc. It can be extremely easy for a computer manufacturer to start a rumour that would compromise a certain type of processor. The beneficiary cannot test the product immediately, and it can take a long time to prove the contrary.

When this kind of warfare extends at the level of the industry branch, against global economic forces or on some states or group of states, we are dealing with a *global information warfare*.

Imagological information warfare is not necessarily intended to gain information superiority but to manipulate the enemy or own population with false or altered information through TV shows, video tapes, photos, and more recently through the internet.

Even the church is influenced by the effects of this phenomenon, therefore, at the Vatican, there are two kinds of priests, in white robes and in black robes. If those in white robes are involved in public relations, speaking of peace, freedom, democracy and unity, having diplomatic relations with all governments of the world, the priests in black (man in black) are *“behind the scenes”*, they are among the leaders of the Jesuit Order, who lead the vast Catholic institutions across the globe (including astronomical observatories and control of high technologies); through them, the Vatican controls all education aspects worldwide. They are secret intelligence, *“weapons”* of the Jesuit espionage.

In specialised literature, it is considered that *information warfare* uses *“weapons that do not kill”*, designed by their users to *“reach goals in those situations where the use of traditional weapons is not accepted out of political or ethnic reasons”*³.

One must not however forget that the binomial *security – insecurity* in the contemporary international environment is *“like in a balance, in which the two <arms> are always in a precarious equilibrium”*⁴.

Even if they have modern intelligence technologies, professional information structures, even if they carry out systematic actions of information warfare, developed states are, in their turn, targets of other states, terrorist organisations, individuals performing daily attacks on government information systems and activities against the interests of those states.

Pentagon revealed that, on 15 July 2011, it suffered one of the largest information losses, when a foreign secret service managed to steal 24 000 files from a US military contractor, following a cyber attack, as reported by *The Daily Telegraph*. This theft is a dramatic illustration of the increasing difficulties faced by the Pentagon to protect secret information. A recent estimation shows that intellectual property and government and commercial computers information theft is estimated at over 1 000 billion dollars.

According to the US National Counterintelligence Executive, the *“most active and persistent perpetrators of economic spying are the Chinese”*. Russian intelligence services seek, in their turn, *“to obtain economic information and technologies to support Russia’s development and security”*, according to the same source.

³ *Ibid*, p. 47.

⁴ Constantin Hlihor, *Politici de securitate în mediul internațional contemporan*, Editura Universității Naționale de Apărare “Carol I”, București, 2007, p. 6.

Knowing that such actions are difficult to detect, and once detected they are not made public immediately, we will present below some of the scandals in this area that have made the headlines over the years:

- ❖ The director of a German company that builds satellites argues that France is the champion of Europe in industrial espionage, “*an empire of Evil in terms of technology theft*”.
- ❖ In the Lopez deal, an employee of *General Motors* is accused of going to Volkswagen with a bag full of secret industrial documents. Four years later, the conflict was resolved amicably.
- ❖ In 2006, two men took possession of the secret *Coca-Cola* manufacturing recipe through an employee of the company, with the intention of giving it to the rival company, *Pepsi*. Upon receiving the capture, *Pepsi* immediately informed *Coca-Cola*.
- ❖ In 2007, the designer of the *Ferrari* single-seater cars communicated the plans to the Anglo-American opponents at *McLaren*. The latter ones were, in turn, involved in a similar espionage action with *Renault*.
- ❖ In 2007, an employee of *Michelin* tried to sell confidential information to competitors from *Bridgestone*. Warned in time, *Michelin* set its employee a trap to catch him in the act.
- ❖ In 2009, the *Hilton* hotel chain was suspected for paying two employees at *Starwood* in exchange for industrial information. The two left from *Starwood* with 100 000 files regarding a project that *Hilton* was preparing to launch.
- ❖ *GhostNet* (2009): it was a vast operation of infiltration in the private PCs network, including security systems, all controlled by China.

National Security and Romanian Espionage

At international level, one speaks more and more about affecting the national interests of states by non-violent and invisible actions, in which the primary place belongs to *information warfare*.

Renowned political scientists and historians have shown that intelligence agencies are vital for the state, for the procurement of information and in order to protect the interests of that state. However, when these huge institutions place themselves at the service of politics, the results are disastrous. Enrolled, they become sources of terror, repression, extortion, passionate repercussions, corruption, political police, generating totalitarian regimes.

As such situations are not forgotten, throughout history, Romania has been, in its turn, dependent on these services, which have evolved at the same time with the Romanian society.

The first institutionalised intelligence structures appeared in our country at the moment of the modern Romanian military organisation, after the Union of the Principalities – 1859. As the War of Independence proved that data collection activities were deficient, with the establishment of the Superior War School (1889) it was also introduced a specialised course – *“Intelligence Service”*.

However, on the eve of the First World War, the Romanian intelligence services had big flaws, and their inefficiency has turned Romania into a heaven of agents sent by the Central Powers, to which was added the poor counterintelligence training of the population, the typical Romanian chatter.

In January 1913, the Romanian Parliament drew up the *“Law on peacetime espionage”*, immediately promulgated by King Carol I, but which stipulated extremely mild sanctions for the spies acting against the interests of the Romanian state: correctional prison from 1 to 5 years or a fine of 500 to 5 000 lei!

A special experience in this field is the establishment of the so-called *“Delta Intelligence Service”*, led by Mihail Moruzov, who, before becoming *“inconvenient”* for the existing political regime at the time, had a significant contribution to the development of the Romanian secret services in the interwar period and the beginning of the Second World War. Although he graduated from only three high school classes, as both his supporters and detractors mentioned, Moruzov was born for intelligence. He began in 1909 as a special agent in the General Directorate of Police and, going through all the steps, on 1 May 1925 he became the head of the new Secret Intelligence Service.

The fact that he came into conflict with Ion Antonescu, gathering compromising materials and records about the enemies of King Carol II, and his conspiratorial attitude made many people label him as *“evil genius”* or *“gray eminence”* of the time.

After the Second World War, under Soviet occupation, the largest civilian intelligence service ended its activity and, under the coordination of Soviet counsellors, the General Directorate of People’s Security (DGSP) was established. Thus began the long night of repression...

Currently, our country’s geostrategic position at the crossroads of several worlds (the former Soviet Union, Turkey, the Black Sea area, the NATO and EU border), the efforts made for Euro-Atlantic integration, the steadfast policy to maintain internal and regional stability, as well as the participation in missions in theatres of operations attract not only appreciations but also hostile actions. Regarding these defamation actions, the Romanian Intelligence Service Director said in an interview for the newspaper *“România Liberă”* on 24 October 2011 that the interest of foreign agents in Romania grew exponentially in the last year.

It had a “*qualitative growth*” especially after the Romanian-US missile shield agreement was signed. It is estimated that, every month, Romania deals with hundreds of thousands of cyber incidents. Yet, many of the vulnerabilities seem to come from within, from the existing mafia clans throughout the country, which make the “*black economy*” represent 25-27 percent of the total economy.

The espionage scandals in which post-revolutionary Romania was involved were aimed generally at a restricted geographical area, Eastern neighbours being involved – Ukraine, Russia and Moldova. The Russians are “*more interested in the topic of NATO*” on the Romanian territory. Referring to this, Iulian Fota, the Romanian President’s Security Adviser, said in an interview given to the newspaper “*Ziua*” on 10 June 2009: “*It is obvious that, from the point of view of certain non-Western entities, we are attractive as target and objective, on the two coordinates: access to information or our attitude in NATO and the EU, which can be influenced by illegal, unorthodox means, including or especially at the political level*”.

Therefore, this activity has never stopped, hence the fundamental principle according to which “*information warfare is a permanent one*” and it must be implemented in security doctrines, by raising real “*walls of defence*”, at several complementary levels that should protect national structures and capacities.

The current intelligence structures carry out supported actions for the annihilation of any attempts to compromise national interests, but Romania’s counterintelligence defence is not a restricted activity, performed only by a number of intelligence officers, but must be a “*national strategy*” involving all citizens. Nevertheless, for citizens to be involved, they must be informed and educated in terms of counterintelligence.

*

We may reckon that domestic and international politics are actually two different manifestations of the same phenomenon: *the struggle for power*. History shows that the nations involved in international politics are undergoing continuous preparation, and in this respect, intelligence services may have a decisive role in staging certain “*incidents*” that may affect certain countries, while others consolidate their power and image as an actor in the international arena.

The power of a nation depends not only on the ability of diplomacy and the military power, but also on the attractiveness exerted for other nations by the political philosophy, but especially the security institutions and strategies applied by this nation.

Of special importance in deciphering the potential of an actor is defining and identifying sources, as well as knowing the sort of *power means* it promotes in international relations.

The new military concepts and technologies are continuously developed and experienced and are meant to completely revolutionise the relations and showcase these *power means*.

There are numerous indicators that raise the possibility of a new scientific revolution in the field of information processing. The use of new technologies for carrying out information attacks makes possible the blocking of the function of public structures, both the administrative and the productive ones. The attacked state can no longer exert its power, control its resources, and provide its citizens with a normal social climate. This new generation of information attacks would enable the pressure on any state through the information control of decision-making centres.

Furthermore, information warfare is rather inexpensive compared to others, allowing developed countries and interested terrorist groups to acquire capabilities in this domain and use them in accordance with their goals.

BIBLIOGRAPHY

1. Barry Buzan, *Popoarele, statele și teama*, Editura Cartier, Chișinău, 2002.
2. Florian Gârz, *Spionajul și puterea*, Editura Obiectiv, Craiova, 2003.
3. Henry Kissinger, *Diplomația*, Editura Bic All, București, 2002.
4. John J. Mearsheimer, *Tragedia politicii de forță*, Editura Antet, București, 2003.
5. J. Hans Morgenthau, *Politica între națiuni*, Editura Polirom, 2007.

English version by
Iulia NĂSTASIE

INTELLIGENCE

– Coordinate of National and Global Security Equation –

Colonel Ovidiu FRĂȚILĂ
Lieutenant Colonel Iosif SOLOMON

Regardless of controversies, different conceptual approaches, and substantive and formal changes in the intelligence activity, intelligence professionals, historians, political scientists, sociologists and policymakers agree on only one aspect: the possession of valuable information is as important now as it was two thousand years ago, and the rapid and profound changes in the global environment require flexibility, accuracy, increased capability of forecasting and acting, and especially structures able to cope with the new intelligence requirements.

The author considers that not all intelligence professionals value scientific and theoretical approaches to intelligence activities, although they may represent a necessary foundation of doctrinal changes and bureaucracy reduction in intelligence services.

Keywords: *information networks; Iron Curtain; information sources; Cold War*

In the opinion of security experts, the modern concept of *security* includes five cumulative factors, the security of a state entity being ensured if each of the following five components is considered: *political, military, economic, society* and *ecological*. The issue of security is not confused with the normal functioning of the state on these dimensions, but refers only to the threats that, by the five dimensions mentioned above, jeopardise the existence of the state itself. **Political security** refers to the organisational stability of states, government systems and their ideologies. **Military security** is related to the interconnection between the level of offensive weapons and the one of the defensive capabilities of states, together with the perception of states about the intentions of other participants in the international area. **Economic security** focuses on access to resources, financing and markets necessary to sustain acceptable levels of development and power of the state. When speaking of **society security**, we refer to maintaining, within acceptable conditions

Colonel Ovidiu Frățilă, Lieutenant Colonel Iosif Solomon – the General Staff, the Ministry of National Defence.

that enable the evolution process, the national collective identity, traditional models of language, culture, religion and customs of a people. Considering the way events take place, some of the biggest problems for European security will be raised by the society component, due to the situations created in Bosnia-Herzegovina, Transnistria, Macedonia, Kosovo, Belarus or Montenegro. **Ecological security** regards the preservation of the planetary biosphere, as an essential support for the system on which all the other human activities depend.

Also, one of major transformations of the current international system is rethinking the fundamentals of the concept of power and its way of exerting power. The logical consequence, taking into account Clausewitz's theory, according to which war is the continuation of policy with other means, is to transform the war into more subtle forms of aggression, with a huge impact on a nation, at all levels: political, economic, social and information.

Semantically, security means "*being protected from any danger*" or "*the feeling of trust and tranquillity in the absence of any kind of danger*", coming from the Latin *securitas*, *-atis*, meaning "*carefree*". More elaborately, security means the premises and circumstances determining the sense of trust, tranquillity, protection and defence against a danger, as well as the measures that lead to preventing any danger.

Clarifying the concept of security was possible when the notion acquired a normative sense. Thus, there was an increase in complexity, determined by the emergence of a series of factors (political, economic, military, information etc.) whose interaction has generated the present concept structured on many levels: human (individual) security, national security, international security, regional security, global security etc.

According to the Explicative Dictionary of the Romanian Language, *national security* means the generalised state of tranquillity and trust that the existence of a nation is beyond any danger¹. In a more applied definition, the National Security Intelligence Doctrine² defines national security as "*the state of a nation, social communities, citizens and state, based on economic prosperity, legality and socio-political stability, expressed by the rule of law and ensured through economic, political, social, legal, military, information etc. actions, with the purpose of freely exerting the citizens' rights and liberties, the free manifestation of the freedom of decision and action of a state, its fundamental attributes and the quality of subject of international law*".

The *national security* syntagm has as fundamental strategic components national defence, national safety and public order. Initially, it meant all the concerns

¹ *Dicționarul explicativ al limbii române*, Editura Academiei, București, 1998.

² Adopted in the meeting of the Supreme Council of National Defence on 23 June 2004.

strictly regarding territorial defence, using conventional means, taking into account that, for a long time, the main factors generating insecurity were military conflicts. Gradually, the concept has been broadened, the globalisation of threats to security bringing about the need for looking for appropriate responses, as a consequence of noticing that military defence does not match the extremely complex issue of ensuring the security of a nation.

The concept of security should be seen in correlation with its associated notions, such as: national interests, national security system and institutions, national security strategy, security means and policies, national security policy objectives, national security principles etc. This correlation allows for a systemic approach to the concept, because it involves multidimensional existence and analysis, among which one may frequently find the political, military, economic, information etc. dimensions. State is seen as the main generator of security, which can be ensured in optimal circumstances only in the case in which these dimensions (sub-systems) place themselves and work interdependently in a security system.

Intelligence services are one of these subsystems, whose main *raison d'être* is to provide national security; they are part of a special sector of state activity, thus resulting a strong imperative for classification. Their unique characteristics provide them with the possibility to act independently, to threaten the position of members of governments, parliamentarians, politicians and to jeopardise democratic governance, fundamental rights and freedoms of citizens, which may result in a dysfunctional democratic system.

Mark Lowenthal defines *intelligence* as a³:

- *process* – the means through which certain information types are required, collected, analysed, protected and disseminated, as well as a coherent ensemble of methods and procedures, legal and illegal ones, open or covert, used to attain the purpose;
- *product* – the end result of the process;
- *organisation* – the structures, units, organisations that implement the process and provide the product.

The state is seen like the main promoter of security, which can be assured in optimal conditions only if these subsystems can operate together inside the security system.

³ Mark Lowenthal, *Intelligence: From Secrets to Policy*, Washington DC, Congressional Quarterly Press, 2002.

The information is pursued by all the components of the international system. The international system could not work without information, the levels of the system interact and survive through information.

The purposes of collecting and gathering information are different, though (as, in fact, the means, methods of obtaining it); they can be of domination, control or survival.

Throughout centuries, any paper regarding history, political sociology, governance, even political philosophy, from Sun Tzu, Machiavelli or Hobbes⁴ until today, has dealt with the intelligence issue as a subject connected to the area of study, considering it *knowledge and analysis design to assist action*⁵.

The importance of studying intelligence has never been more significant like in our days. For example, declassifying the *Cold War* archives, the terrorist attacks on 11 September 2001 and 11 March 2004, the media scandals of the Gulf War and the military interventions in Iraq and Afghanistan, the change in the paradigms of the national and international security have produced major changes in the way the intelligence issue is studied at academic level.

Intelligence, the information in any state, is part of the arsenal of the new asymmetrical conflicts. The possession, power and use of intelligence are the stake of the asymmetrical conflict. Shaping themselves in keeping with the new information features of information society, intelligence services must redefine their goals, strategies, doctrines, identify the new forms of threats and the ways to prevent them.

Security is no longer defined by means of military parameters. The security of a nation refers today to democratic security, economic security, information infrastructures security, individual security. The immediate effect of the change in the security paradigm at internal level has been the transformation of the role and share of intelligence in the decision-making process, the political action being more and more based on the quality and quantity of intelligence products.

Topics such as security and intelligence are present more than ever in the political speeches and the public awareness.

In 1976, British Prime Minister Harold Wilson said that it was dangerous and inefficient for the general national interest to publicly discuss about security and intelligence issues; today, for the first time in the history of British secret services,

⁴ Thomas Hobbes, *De Cive*, Cambridge University Press, 1998.

⁵ Robert Bowie in Ernest May, *Knowing One's Enemies: Intelligence Assessments before the Two World Wars*, Princeton UP, 1984, p. 3.

their utility and role in the political action at international level are openly affirmed, and the US President spends an hour every morning with the chief of intelligence and the security adviser.

We will make a brief history of the main disagreements and issues implied by our attempts to academically approach the study of *intelligence*.

If the success in this activity remains mostly unknown, failures have an overwhelming effect on the political, social and economic area. We can compare the impact of intelligence failure with the force of a tsunami due to the incomplete information, the variety of the sources who “*reveal*” it and the publishing of new theories of conspiracy.

Any intelligence failure provides new opportunities for political parties to confront and find “*guilty sides*”.

The success of the *intelligence* work contributes to the stability and security of a nation but, at the same time, in what way does its failure affect the internal policy and the public trust in state institutions?

The trust in individual security, in the capacity of the state to defend its citizens has decreased and that develops psychological trauma which brings discredit on intelligence services or, quite de contrary, the rise in its power and functionality.

The psychological trauma suffered by Americans – the most important being becoming aware of their own vulnerability and the fall of the myth of the superpower protected from any direct attack – has changed the public perception regarding secret services and law changes, seen by specialists as signs of a totalitarian system.

Five decades ago, Sherman Kent⁶ studied for the first time in a scientific manner the issue of intelligence, in his work paper “*Strategic Intelligence for American World Policy*”.

In the '80s, two British scientists, Christopher Andrew and David Dilks, mentioned for the first time *intelligence as a stand-alone dimension of international relations*, underlining the compulsoriness of studying intelligence in this context⁷. While the other political sciences upgraded their concepts, for intelligence the concepts were old and non-applicable.

⁶ Sherman Kent, *Strategic Intelligence for America World Policy*, Princeton NJ, Princeton University Press, 1949.

⁷ Christopher Andrew, David Dilks, *The Missing Dimension: Governments and Intelligence Communities in the Twentieth Century*, University of Illinois Press, Urbana IL, 1984.

The social, cultural and technological changes have also imposed the need for radical change in the area of concepts, methods and ways as well as in the organisational structure. The multiplying and diverse threats to the nation state, the emergence of new state competitors on the global arena and the rising danger of the threats coming from non-state actors must have as response some changes in the organisation of secret services and in the popular perception of intelligence and the necessity for these activity⁸.

In the debates on approaching the study of the theory of international relations created between liberals, conservators, realists and postmodernists one will not find the subject of intelligence addressed as a fundamental element in the coherent construction of foreign and international security policies.

It is interesting to underline that, though the study of intelligence is part of the theory of international relations, the neorealist writers have ignored the academic approach to intelligence.

With all the recognition of the importance of studying intelligence, in 1992, James Der Derian wrote: "*intelligence is the least understood and most under theorised area of international relations*"⁹. The link between intelligence and political strategy becomes clear when things are changing, when a cycle ends and another begins, which require the change of old paradigms (the completely changed relations between the USSR and the USA at the beginning of the Reagan Administration, the emergence of new economic and nuclear competitors, the disappearance of the ideological conflict and the shift of the conflicts in the religious, cultural and ethnic areas, the recrudescence of the Islamic fundamentalist terrorism etc).

The academic studies regarding intelligence conducted lately have proved that it is necessary that intelligence is studied in any approach to the theory of international relations, governance studies, the way in which political decision affects good functioning of a society inside it or in the relations with other global actors.

Michael Fry and Miles Hochstein pointed out, in 1994, that, even if the study of intelligence increased and it had a multidisciplinary approach, it was not integrated in an academic manner in the studies regarding international relations¹⁰.

⁸ Andrew Rathmell, *Towards Postmodern Intelligence*, in *Intelligence and National Security*, vol. 17, no. 3, 2002, pp. 87-104.

⁹ James Der Derian, *Anti-Diplomacy: Spies, Terror, Speed and War*, Oxford, Blackwell, 1992.

¹⁰ Michael Fry, Miles Hochstein, *Epistemic Communities: Intelligence Studies and International Relations*, in *Intelligence and National Security*, vol. 8, no. 3, 1993.

The declassifications in the last decade determined a different approach to the activity of intelligence, although the perception of the population towards the role played by intelligence is, in most cases, wrong. One of the few subjects regarding which specialists have similar opinions is the one of the *need for social recognition* of the utility of intelligence services and of intelligence in general. Nevertheless, the way the process of social recognition can be improved is dealt with differently, depending on the professional area of the one approaching this topic.

Historical research can be used to support the effort of social recognition of intelligence.

Christopher Andrew wrote, in 1997, *“Intelligence Agencies that ignore their past are as vulnerable as people who lose their memory”*. Declassifying intelligence services and studying intelligence archives will make it possible for rigorous analyses to be made regarding the efficacy and utility of intelligence estimates in the political decision-making process and the way in which the intelligence community has collected, processed-analysed and spread the information.

Among specialists, there are often controversies regarding: the definition of the concept, information flow, utility and users of intelligence and study methodology.

Unlike the domains it is partly related to, history or political science, intelligence is not an independent intellectual domain. The declared purpose of the intelligence area of study is not necessarily searching for the truth, but enabling the decision-making process regarding the domestic/foreign and military policy. This is the practical feature and the *raison d’être* of intelligence.

For us, it is difficult to work with this concept without an appropriate term in the Romanian language. In the political theory literature, in strategy and state politics, intelligence is used with the meaning of *“knowledge of events, tendencies and personalities that may affect the observer or country, institution or governmental service for which the observer works, in an immediate situation or perceived like immediate. Such information identifies, describes and defines situations that require and/or seem to require decisions”*. Essentially, it means information collection and analysis activities in order to support the policymaking process with the purpose of substantiating or adjusting national security strategies¹¹.

¹¹ Amos A. Jordan, W.J. Taylor, Jr., Lawrence J. Korb, *American National Security. Policy and Process*, The John Hopkins University Press, Baltimore and London, 1989.

In our specialised literature, *“the intelligence administrated by the structures with responsibilities in the field is intelligence for national security... and represents the ensemble of new data, documents, objects or activities, no matter the support, shape, meaning or distribution... and is the basis for making decisions by national security specialists and enables the knowledge and evaluation of the operative situation”*¹². Rather vague and general, including a large amount of contradictory concepts, the definition above contributes to pointing out the need for the conceptual and doctrinaire study in a multidisciplinary, complex and modern manner. The first step to clarify the concept was made by adopting the *National Security Intelligence Doctrine* (2004), which explained that *“on the basis of an approved doctrine, it will be very possible to reevaluate the security strategies and intelligence system, as a state feature and as a career...”*.

What does intelligence mean? How can we define the intelligence activity? Should we make a difference between covert and open source intelligence within the intelligence concept? Should the use of intelligence by the decision-making factors be included in the information cycle diagram? What are the differences between intelligence and the other information collection activities carried out by other governmental organisations? In which way is the internal and international policy agenda affected by intelligence activities? Is there a propensity of certain politicians for using the intelligence and how does this behaviour affect the activity of intelligence services?

These are questions in a debate between scientists, historians and intelligence professionals that have not got clear answers yet.

The entire theoretical construction of Michael Hermann, *“Intelligence Power in Peace and War”*¹³ is gathered around the idea that intelligence represents a form of state power. Other political scientists¹⁴ see intelligence not like a form of state power but as a tool necessary to impose state power.

The approaches of sociologists and political science specialists are based on the idea that the utility and efficacy of intelligence are deeply affected by the quality of political leadership, their perception on the value and limit of intelligence and their own political agenda.

The relationship between political leaders and their advisers on security matters is under the public and media attention.

¹² *Profil Review*, publication of the Intelligence Romanian Service, no. 10, March 2006, p. 20.

¹³ Michael Hermann, *Intelligence Power in Peace and War*, Cambridge University Press, 1996.

The relation between intelligence and policymaking has been always recognised, yet, until today, it has not been studied carefully by focusing on the way in which the political tendencies affect the intelligence process – the search for information, its analysis. Moreover, because of the classification of information, the research of the impact of intelligence on changing attitudes and actions among political leaders has not been possible.

The closeness between the political leadership and the intelligence services is another field that deserves to be studied more. Political leaders who came from intelligence structures funded their decisions on intelligence products (Andropov, Bush); other political leaders showed a large interest, even passion towards the intelligence activity (Margaret Thatcher, Francois Mitterand) or mistrust (J. Carter, Helmut Kohl).

However, all of them agree that the difficulty in having a general theory concerning intelligence results from the fact that *the role and the utility of intelligence are strictly related to the interaction between producers and consumers of intelligence*.

Michael Hermann has asserted in his already mentioned book that the quality of the intelligence product could induce a growth in the consumer's trust, without any guarantee regarding the growth of the influence of intelligence on the decision-making process. The ability of the consumer to use an intelligence product is not necessarily related to their nature – prejudices, intellectual and cultural level, personality – but to the political, military, economic and social factors.

The classic form of the intelligence cycle: to search – to collect – to analyse – to disseminate is completed by the *intelligence* user, presented as an external point of the *intelligence* process¹⁴, without explaining the way in which the intelligence product becomes part of the decision-making process or the way in which the political action resulted from delivering certain may trigger, in its turn, a real feedback having the capacity to change all the *intelligence* process. As any system, the intelligence system needs a self-adjustment, which means the existence of an adjusting feedback, an aspect very superficially studied.

Studying the feedback of *intelligence* and its consequences for the different stages of the information cycle is one major step that must be taken for a correct definition of the *intelligence* concept.

We can consider the decision-making process as the *black box* and the *intelligence* as one of the inputs. The efficacy of intelligence is maximal

¹⁴ John Ferris, *Intelligence*, in R. Boyce, J. Maiolo, *The Origins of World War Two*, Palgrave, 2003, p. 308.

¹⁵ Amos A. Jordan et al, *op. cit.*

when it determines a change in the output – the political decision-making – when the other inputs remain unchanged. In reality, it is very difficult to sustain this functioning state of a system. Therefore, how do we measure the utility, the efficacy of intelligence?

In most cases, the efficacy of intelligence is measured post factum. Studying the course of events can prove if the intelligence product has determined a political decision to benefit the national interests. Nevertheless, can something that seems, at first, a “*politically correct*” decision, based on a valued *intelligence*, turn into a decision-making failure?

Another aspect that brings many contradictions is related to the lack of concept concerning the differences between the intelligence process and the activity of other governmental agencies for intelligence. Especially in the last decade, there were many non-governmental private entities (led by former intelligence professionals) which deployed specific intelligence activities in private or official purposes. In this context, Michael Hermann’s¹⁶ solution through which he identified the intelligence with specialised, governmental organisations whose name includes the word intelligence, which were involved in the intelligence activity, having intelligence as the “*end product*”, is not enough anymore.

Different approaches will also be found out in the matter of *intelligence sources*. If most pieces of information are provided by open sources, in which way does this modify the concept of *intelligence*?

This question is legitimate, since specialists like M. Hermann, when speaking of open sources, name them “*non-intelligence sources*”.

Moreover, the use of the Internet and the information infrastructure changes the intelligence approach, because it is not only an open database, accessible to the public, but also a good field for gaining access to confidential information. The computerised network of the United States Intelligence Community represents a vulnerable area and “*the richest treasure for espionage*”¹⁷. The use of new information techniques has gained ground among intelligence specialists, as well as military and industrial espionage, illegal banking transactions of terrorist cells.

The large IT infrastructures in Western states encourage the hacking phenomenon, the effect of a classical terrorist attack having a huge impact if it is doubled by computer hacking attacks.

¹⁶ Michael Hermann, *Diplomacy and Intelligence*, in *Diplomacy and Statecraft*, 9/2, 1998, pp. 1-2.

¹⁷ John Ferris, *Netcentric Warfare, CAISR and Information Operations: Towards a Revolution in Military Intelligence?* in *Intelligence and National Security*, vol. 19, no. 2, 2004.

RMA (Revolution in Military Affairs), NCW (Network-Centric Warfare), CAISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance), IO (Information Operations) are terms employed by any member of the United States Intelligence Community.

For the first time since the end of the *Cold War*, the *Secret Intelligence Service – SIS* and the *Central Intelligence Agency – CIA* recognise the deficiency of the intelligence sources in terms of quality given the circumstance of the worldwide spreading threats. Secret services always had to substantiate their intelligence reports on sub-source information or on pieces of information which, because of too long source-beneficiary chains, lose credibility and are very difficult to verify.

Immediately after the fall of the *Iron Curtain*, the activity of intelligence agents came under the influence of the Hilton effect, typical for journalists (journalists exchanging information on hotels corridors without verifying it).

Being under the pressure of intelligence emergencies, beneficiaries and generations changes, intelligence services have increased their productivity to the detriment of quality. The intelligence penetration of Islamic fundamentalist structures and of terrorist organisations has proved to be a difficult task even for the *CIA* or *SIS*.

In the process of *rethinking of the work with agents and collaborators*, one can notice a more frequent orientation towards hunting information instead of gathering/collecting information¹⁸.

Having as a model the new characteristics of a computerised society, intelligence services must rebuild their objectives, strategies, doctrines and identify the new forms of threat and the ways to stop them.

The *human resources management* of intelligence services is about to change; the new recruitment policy lays a large stress on the language skills and the origin of the future employees in terms culture, religion etc.

No matter the controversies, different ways of approaching intelligence, there is one aspect upon which specialists have agreed: possessing valuable information has the same importance as 2 000 years ago; the rapid and deep global changes require flexibility, accuracy, a high capacity of predicting, acting and, mostly, specialised structures capable of facing the new intelligence requirements. Most intelligence specialists do not consider important the scientific, theoretical researches on the intelligence activity. However, the academic approach to intelligence,

¹⁸ Charles Cogan, *Hunters not Gatherers: Intelligence in the Twenty-First Century*, in *Intelligence and National Security*, vol. 19, no. 2, 2004.

the intelligence studies regarding its power and use could represent a daily support, a basis for a new doctrine and the decrease in the bureaucracy within intelligence services. A veteran of the American Intelligence Community said: "...the agencies need a shift in priorities with less focus on the gathering of information and more focus on the harder job of providing insights into what that information means"¹⁹.

Security and Intelligence in a Democratic Society

Considering the importance of ensuring national security for the good functioning of any society and the essential role played by intelligence services in the process, it follows that the major challenge to controlling and supervising the activity of intelligence services is posed by the imperative of balancing the need for security and the public interest with the individuals liberties and rights specific to a democratic society.

The interest of the state to have efficient intelligence services overlaps with the citizens' interests to be protected by the legal intelligence services, functioning in keeping with democratic rules and standards, but sometime comes into conflict with the democratic value of individual liberty.

The main reasons for a parliamentary democratic control over intelligence services were revealed in a study regarding the oversight of intelligence services, written by Hans Born and Ian Leigh²⁰, and are presented below.

First of all, the activity of intelligence services is secret, avoiding the public exposure and evaluation. Therefore, it is important for the Parliament to monitor the intelligence services operations.

Secondly, by their statute, the intelligence services have special abilities, like the possibility of intercepting the communications, which can limit the human rights. In order to prevent such situations, the parliamentary control is necessary. Mention should be made that the mission of parliamentary control over intelligence services is also supported by international and European forums. For the past years, more and more organisations have agreed upon this process. International forums such as the Inter-Parliamentary Union, Council of Europe Parliamentary Assembly agree that intelligence services must be under a democratic control.

Thirdly, the post-*Cold War* period and especially the 11 September 2001 events marked major changes concerning security threats. The main threat for democratic

¹⁹ Loch K. Johnson, *The CIA's Weakest Link: Forget James Bond. What Our Intelligence Agencies Need are More Professors*, in *Washington Monthly*, July-August 2001, p. 6.

²⁰ Hans Born and Ian Leigh, *Making Intelligence Accountable: Legal Standards and Best Practices for Oversight of Intelligence Agencies*, Norway, 2005.

societies was not a foreign military intervention, but the risks represented by terrorism, organised crime, regional conflicts, illegal human, weapon trafficking etc. This evolution of the security environment has required that intelligence services readapt their activity to the new threats, a process that has taken place under the control of civilian authorities, which are the only ones to guarantee the equilibrium between the needs of citizens and the changes in intelligence services. Moreover, the parliamentary control must make sure that the planned changes are implemented in an efficient manner.

Another important aspect is represented by the fact that, in general, intelligence services must collect and analyse the information on possible threats and evaluate the possible risks. To evaluate the risks, which is the starting point for the other security forces of the state – means to prioritise the threats that usually have significant political consequences. That is why it is necessary for the entire process to take place with respecting the principles of parliamentary control.

The last reason is specific to the states that passed from a totalitarian political regime to a democratic one. That means a long process to turn a repressive intelligence service into a democratic and modern one, under the control of the Parliament.

In general, the security culture is a way to present reality in relation to individual and collective security, by the already mentioned means. At national level, it also represents the preparation of the entire society for defending the country, respecting the law and national values, traditions and customs, in order to counteract a possible internal or external adversary, being an example of education, morality and good behaviour. No matter the environment in which the action for providing a state of security takes place, the end beneficiary will always be the citizen. The citizen, as an individual belonging to a community, must be prepared and trained in the security field in order to contribute to building the security climate and to receive and appreciate in a right way the security values.

Today, we are witnessing a broad process of contamination of the popular language with the disease we call *intelligence-itis*, similar to *management-itis* and *policy-itis*. No matter insignificant an activity is, it is *managed* with the support of a *policy* based on appropriate *intelligence*. Therefore, this is another reason for correctly defining and understanding the terms employed and their impact on the society.

The simplest definition for *intelligence culture* must contain all the defining elements of the concepts that form this syntagm. Thus, it can be *a way of representing reality in relation to individual and collective security, through a complex of knowledge, norms,*

values etc. related to the processes, products and organisations in the intelligence field.

The syntagm *intelligence culture* could be defined as an “ensemble of laws, concepts, beliefs, values, traditions and moral behaviours through which the people, other than those working in intelligence services, are prepared to ensure, in peacetime and at war, the protection of national values, history and traditions against a potential adversary, from the perspective of the intelligence activity”²¹. Moreover, *intelligence culture* in the military field is defined as an “ensemble of laws, concepts, values, traditions, beliefs and moral behaviours through which the military are always ready to ensure, in peacetime and in conflict situations, the protection of European, national and military values against a potential adversary, to use efficiently the pieces of information and intelligence products to make decisions and to communicate in due time the information obtained”²². Both definitions refer to the operational aspect, which means the implementation of the elements of the security culture.

The existence of the intelligence culture must be understood and accepted within the broader sense of the security culture. These two concepts often intermingle, and the purpose of this article is drawing clear lines of demarcation especially because it does not exist in the common meaning of the terms. Quite the contrary, many of the ideas and actions related to the existence, formation and development of security culture are presented precisely because they represent, in fact, notions or processes collected to the intelligence domain.

WEBOGRAPHY

1. http://intellit.muskingum.edu/reform_folder/reformtoc.html
2. <http://www.fas.org/irp/commission/htm>
3. www.tandf.co.uk/journals

²¹ Florin Lungu, *Rolul educației de securitatea informațiilor în cultura de intelligence*, in *Adaptarea serviciilor de informații la schimbările mediului strategic – o privire în viitor*, Scientific Papers Session of the Defence Intelligence General Directorate, November 2011.

²² Nuță Dragomir, *Cultura de intelligence în domeniul militar*, in *Infosfera*, no. 4/2010.

INTELLIGENCE SERVICES AND EARLY WARNING

Lieutenant Colonel Cătălin BALOG

Motto: "History is a vast early warning system"¹.

Norman Cousins

One of the outcomes of intelligence activities should be, in the author's opinion, to permanently issue signals and warnings to provide a timely, comprehensive and truthful flow of information about the intentions of potential enemies and allies, so that decision-makers can substantiate, in due time, an action strategy in keeping with the state/nation interests and aspirations.

The delays and gaps in this flow may result in circumstantial measures, adopted after the outbreak of events, which may lead, in the case of limit situations, to the severe damage of the state/nation interests for a long period of time.

Keywords: *intelligence; analysis; early warning; early response; decision*

❖ **Early Warning**² – *EW* is the decision-makers warning process regarding a prospective outburst, beginning or taking over of violent conflicts³ and promoting the understanding between decision-makers as to their nature and impact.

The first suggestions related to an early warning system were made by the United Nations High Commissioner for Refugees – *UNHCR*, Prince Sadruddin Aga Khan, in 1981, in the Report called *Massive Exodus and Human Rights*. A step forward was done by setting up the first NGO for preventing conflicts (*International Alert*), in 1985, and its support for early warning. Thus, in 1987, the UN founded *The Office for Research and the Collection of Information (ORCI)*, for developing an early warning system designed for monitoring and analysing global development trends⁴. However, the movement factors that promoted early warning at an international

Lieutenant Colonel Cătălin Balog – "General Nicolae Condeescu" Defence Intelligence Training School, București.

¹ Norman Cousins (1915-1990), political journalist, professor at the California Faculty of Medicine, pioneer of human emotions biochemistry research.

² *Conflict and Peace Analysis Response Manual*, FEWER, 1999.

³ In the context, conflict can be defined as a real situation in which two sides are involved (individuals, groups, countries), which follow incompatible objectives or the same one that cannot be attained except by only one of them or that want to employ means incompatible with attaining a purpose.

⁴ K. Rupesinghe, *Early Warning: Some Conceptual Problems*, in *Bulletin of Peace Proposals*, 1989.

level were *UNHCR* and the *United Nations Office for the Coordination of Humanitarian Affairs* (formerly, *UNDHA* and nowadays *UNOCHA*), supported by the need of precise and proper knowledge regarding the great number of refugees, for planning emergency situations. The end of the *Cold War* had a positive effect upon the entire conflict prevention framework. In the '90s, through the American academic environment, they had a great influence upon the development of analysis methods, more precisely quantitative ones, and, towards the end of this period, a series of conflict qualitative analysis methods appeared promoted by the *Peace Fund*, *FEWER*, *National Bank*, *USAID* (*Agency for International Development* – USA) and *DFID* (*Department for International Development* – UK).

Between 2001 and 2002, a common understanding was created related to early warning characteristics, as follows: • it is located as close as possible to the interest area and it has powerful monitoring networks; • it uses multiple resources including the open source framework for easy access; • it employs a combination of quantitative and qualitative methods; • it uses proper information and communication technology; • it provides regular reports and updates of conflict development, the main national and international actors; • it has links supported by proper response mechanisms. That is why, systems such as *CEWARM* (*Conflict Early Warning and Response Mechanism*), *WARN* (*West Africa Early Warning and Response Network*) and *PHSC* (*Programme for Human Security and Co-Existence* – programme of *FCE/Foundation for Co-Existence*) began to combine early warning and early response, within one system.

❖ **Intelligence Services** are institutions set up for a preventive role, having the following main tasks: • preventing strategic, economic, political, technical-scientific, ecological and any other kind of unawareness and • informing the decision-makers regarding action accomplishments within the security and defence fields. In other words, intelligence services must be one step ahead any kind of military or non-military threat (social-political, economic, ecological crises, ethnical, religions conflicts, asymmetric threats) meant to jeopardise the nation or country.

By specific means and methods – that the judicial system “*more or less*” allows, by using the so-called “*state reasons*” and with the consent of political decision-makers, through whom intelligence services are controlled and managed, making use of political mechanisms of power – the intelligence services can contribute both to preventing and to starting events of tremendous historical importance, based, to a great extent, on the intelligence professionalism as well as decision-makers interests. The historical background proves there were many cases in which intelligence services – skilfully used by the political powers – got involved

in starting events that either influenced the development or contributed to the beginning of military conflicts. Both the First and the Second World Wars could be supporting examples to this.

For preventing strategic surprise as well as informing decision-makers, the intelligence services carry out a quite complex activity. Thus, one of the outcomes of the intelligence service activity should be permanent issue of signals and warnings which could form a timely, wide and trustworthy information flow about the prospective enemy or ally intentions, so that the decision-makers could come up, in due time, with an action strategy according to the interests and plans of the country/nation. Delays or flaws in this cycle can result in actions determined by the circumstances and measures taken after the events occurred. This could lead, in a crisis situation, to seriously harming the interest of the country/nation in the long run. To sum up, it can be said that early warning is a means of action for accomplishing basic tasks of any kind of intelligence service.

Early Warning

❖ Early Warning and Early Response

Early warning systems require a group of organised, ordered and systematic collection and analysis activities regarding the information coming from the crisis areas, carried out for: • anticipation of an escalation of a violent conflict, • development of strategic answers to these crises, • presenting critical actor options for decision-making purposes⁵. These systems provide a set of early warning products based on quantitative and/or qualitative analysis methods usually linked with answer mechanisms and tools.

Quantitative analysis methods greatly contributed to understanding the causes so that some experts consider the level of accuracy as being approximately 80%⁶. Work methodology requires using historical data processing systems and structural analogies and coding up to reaching a highly predictable significant factor. The challenge increases as the data sources needed for identifying the trends are limited.

Qualitative methods came as answers to the deep understanding of the conflict environment and proper response means, by linking analysis to the action planning framework. These methods are used for deep context analyses and the planning methodology of proper reaction to a crisis situation, as well as in the assessment area of conflict response impact.

⁵ A. Schmid, *Thesaurus and Glossary of Early Warning and Conflict Prevention Terms*, FEWER, 1998.

⁶ J.A. Goldstone, *Using Quantitative and Qualitative Models to Forecast Instability*, Special Report, United States Institute of Peace, 2008.

The indicators used in the early warning activity can be prior events, signals; signs used for anticipating and refer to: a) general, structural, fundamental, systemic causes and prior conditions having profound causes; b) connected, specific, situational circumstances and c) direct factors, sudden events (assassination of a leader, election fraud, and political scandal).

Early response systems are mechanisms and instruments having a preventive political, economic and financial, social or security character, activated by early warning, being employed, carried out or deployed for crisis situation management. *Early Response – ER* refers to any action that takes place as soon as the threat is identified and it has the purposes of managing, solving or preventing.

❖ **The Warning Framework**

Warning requires informing the decision-makers on time regarding a potential threat so as a decision could be taken, allowing carrying out efficient counteracting actions. When the intelligence services give a warning about a potential threat, the decision-makers have the chance to take all the needed decisions for cutting down or destroying the threat effects. These actions can be diplomatic or military initiatives, economic sanctions or attempts for influencing the media.

Most intelligence services develop warning policies by which they attempt to avoid false warning of the decision-makers, and thus, of the population as long as there is no information with a high level of certainty for an imminent threat. An intelligence service can lose its reputation by raising a false alarm, while the decision-makers risk subduing the national interests if they wait longer than needed for action. Warning does not mean being right, but being safe. This requires that the warning process is a superior point of understanding of the semantic link between attention and vigilance, and it does not need waiting for completely safe actions. Analysts from the intelligence services – irrespective of their positions – have the responsibility and the duty to inform the management when they notice clues that can have a significant impact within their area of responsibility. It is known that warning must be done on time to avoid surprise, while certain actions, especially the ones coming from the technical-scientific field, are managed rather progressively.

Practically, warning requires careful surveillance, carried out continuously. Analysts within the military intelligence services must focus their attention on the following kinds of warnings: 1) warning regarding general military war action or *warning related to a potential aggression* – being defined as the process of warning decision-makers about aggressive threats coming from an enemy/opponent or the fact that it began a whole set of actions for preparing a potential aggression and 2) *warning regarding a forthcoming attack* – representing timely informing

decision-makers regarding the fact that an enemy/opponent, apart from the fact that it is getting ready for aggression, plans to launch an attack, in the near future.

The most important aspects when taking a decision related to the moment of warning the political or military decision-makers are represented by their effect upon the ones that decide and the chances for a certain event to occur (*example 1*). In case an event that must be reported would take place, analysts should assess its consequences. Any event that may have a moderate to significant impact must be considered. The more precisely the probability assessment outcome is determined, the faster the decisions-makers warning should be (*example 2*). In the end, the decision-makers are the ones who decide what actions must be taken as a reaction to warning, but, ideally, it should be planned (*example 3*).

❖ Warning Principles

According to specialised studies, there are four basic stages regarding the warning methodology: 1) *discovery of a problem that refers to warning*; 2) *its monitoring – the critical indicators that characterise it*; 3) *threat assessment*; 4) *decision-makers warning*.

There are also two kinds of warnings: *strategic* and *tactical-operational* ones.

Strategic warning is defined as being “*a warning prior to the initiation of a hostile act by a country or an organisation*”. This requires indicators that prove that something is to happen, such as the mobilisation of the armed and reserve forces, national campaigns for blood donations, deployment of military units outside their present jurisdiction, unusual security actions, critical resources gathering (fuel) etc. To take part in a war, a country or an organisation must get ready. These things provide the analyst with all the needed elements, based on which they can issue a strategic warning to the decision-maker.

Tactical-operational warning is defined as being “*warning after the initiation of a threatening or hostile act, based on data and information from all available sources*” (*example 4*).

The defining elements that make the early warning process work are the opportunity and taking advantage of this opportunity. Opportunity is used by analysts in issuing scenarios regarding possible actions and events that an opponent can carry out. The emphasis is placed on accomplishing scenarios in which events must be critically interdependent. A scenario does not mean a prognosis, but something built, a pattern that can describe the means in which events happen until the end, the threat respectively. However, to be able to send useful and on time early warning, the analyst must accept sacrificing certainty elements in favour of ones that are related to gaining time in the decision moment. Postponing the dissemination of a warning

analysis until the moment in which new elements come up contributes to reducing the flexibility of decision-makers when counteracting a threat.

Are there any mistakes? There definitely are, but history provided some examples of tragic events in which there was previous evidence but nobody warned the decision-makers in due time (*example 5*).

Nowadays, strategic early warning, regarding terrorism or any other kind of small in intensity but significant incident, is much difficult to accomplish than the one for a conventional military conflict. Present asymmetrical threats are more than a challenge, and issuing warning is much difficult to attain as compared to the conventional threats from the *Cold War* period. The means of using scenarios constructively and imaginatively as well as their proper accomplishment will be key elements in providing strategic warning. The events from 11 September 2001 proved, once again, the importance of strategic warning.

Analysis Activity

❖ Intelligence Analysis and Early Warning

Although early warning is the responsibility of intelligence services, diplomatic missions – from the affected countries – or intergovernmental or non-governmental systems, the initial concept of early warning did not take into account intelligence analysis patterns. Thus, here are certain aspects regarding early warning systems and traditional intelligence analysis systems:

- EW is of interest for intergovernmental organisations that access with difficulty the intelligence area of a member country as compared to another one;
- EW uses transparent collection, analysis and dissemination methods, while intelligence systems are based mainly on classified information and cryptic dissemination;
- EW tends to be decentralised and very dependent on information provided by civil society;
- unlike intelligence systems, early warning involves a closer link between analysis and the action itself, although action intelligence is something wanted by both typologies. In many cases, intelligence and operations are separated, for two reasons: 1) to ensure the integrity and objectivity of the secret analysis, based on classified information, without benefiting from references or external expertise; 2) to be separated from the political side of the intervention, imposed by the fact that the analysis must not reflect the “*the master’s voice*”⁷.

⁷J. Cilliers, *Towards a Continental Early Warning System for Africa*, ISS Paper, April 2005.

In most of the cases, due to the stages the final product of early warning goes through, sources and methodology, early warning systems are similar to analysis ones based on open sources (OSINT)⁸. In the recent years, these systems have undergone institutional, contextual and technical changes. From the institutional point of view, progress has been made regarding international, regional and global conflict response capabilities, in terms of both operational and structural initiatives. In terms of context, we have witnessed changes regarding the kind of real and perceived threats and, consequently, the system topics and objectives have been focused on conflicts between countries, terrorist threats and proliferation of weapons of mass destruction – *WMD*, organised crime, drug trafficking and massive migration. From the technical point of view, as the capabilities and the value of collection and quantitative and qualitative analysis instruments increased, these were integrated in different governmental, intergovernmental and NGOs early warning systems.

❖ Why Do Analysts Avoid Warning?

Warning requires an activity having a continuous and interactive aspect of identifying threats, assessing probabilities and, after that, it involves the warning itself.

Sometimes, analysts avoid issuing warnings, because they consider that their professional credibility is being harmed. The fear of making a wrong suggestion creates inhibition that concludes with anxiety and refraining attitude when promoting certain scenarios that require issuing warnings.

Decision-makers also consider that warning is bad news, starting from the premise that this requires taking unpleasant decisions and limiting future political options. On the other hand, repeated warnings can give the decision-makers a superficiality attitude that can result in ignoring a threat (*example 5*).

Irrespective of the situation, intelligence services, and more precisely intelligence analysts, have the responsibility of alerting decision-makers regarding any kind of threat against national/international security. When this aspect is not confirmed, the intelligence services will definitely be blamed. Despite the difficulty of this responsibility, an analyst's attitude must be proactive and not reactive, this requiring integrity, thorough study, experience, cooperation with decision-makers.

⁸Through open sources, we understand the information that is available – upon request and observation – and any other kind of unclassified information, with limited access or distribution in an unclassified context, without jeopardising the national security, sources or intelligence methods. Mainly, these include traditional and emergency media, internet, grey literature, commercial databases, commercial imagery, experts and observers.

❖ **Challenges and Trends**

The new security environment issues requests, both for the intelligence products and for the action plans, which must shape decision-making projects and simulate the outcomes of decision-making. The global crisis, the overlapping of contradictory processes as well as globalisation and fragmenting, the fuelling of regular tension areas, the encouragement of the trends of geopolitical reconfiguration of certain sensible areas from the Greater Middle East, Africa, Caucasian-Caspian area, Central Asia, the requirements of sustainable security – which require focusing insecurity activators (climate changes, competition for resources, economic, political and cultural marginalisation of most of world population and global militarisation) in the long run – represent real challenges for early warning systems.

One of the greatest challenges is given by *NATO's New Strategic Concept*, a project that suggests a series of military action plans to non-military threats. Thus, governments are recommended to plan emergency situations or interventions as well as to guide intelligence assessments, including regarding climate changes, having related consequences at the level of military planners. The NATO project “*Multiple Futures*” is very useful in this way. This project started in March 2008, as a profound and multilateral examination of the future of the 2030s, having four hypotheses or options of the future: 1) *Future One* – Dark side of exclusivity: it describes the way in which globalisation, climate changes and asymmetry of energy sources greatly affect the countries’ ability to maintain sovereignty; 2) *Future Two* – Deceptive stability: it underlines the need for managing demographic changes resulted from aging population and young immigrants; 3) *Future Three* – Clash of modernity: it refers to a world in which reasoning, along with technological innovation, creates the virtual link of network advanced societies, in the entire world; 4) *Future Four* – New power politics: it describes absolute welfare accompanied by the wide proliferation of methods that create *Weapons of Mass Destruction-Like Effects –WMD/E*.

Nowadays, intelligence services are required to assume more and more the role of early warning systems, by implementing new concepts in the field of intelligence, creating new institutional structures in the field of intelligence along with analysis-synthesis and assessment-estimation development capabilities.

❖ **Conclusions and Appreciations**

Intelligence studies have a short history, the works of the founding fathers being created starting with the interwar period, and the theoretical reflection process coming up only in the last two decades. However, one of the lessons learned by the intelligence services, throughout time, is the one referring

to the need of an own early warning system regarding the means of preventing conflicts and crisis management.

Early warning is not an event, but a cycle in which a crisis, risk, threat are being identified, assessed, defined and for which a list of critical indicators is being made up. Notwithstanding, this is more difficult to accomplish nowadays, taking into account the present features of the international security environment. Critical indicators are continuously monitored and their assessment matrix is always updated. The warning is issued and the cycle is reinitiated.

Early warning can contribute to the improvement of the decision-making cycle, starting with establishing the objectives, developing action plans and their comparison, and, in the end, analysing the action and readjusting it when needed. Thus, due to the early warning function, the specific procedures will focus on data collection, assessment and analysis, starting from the first stages of conflict prevention and crisis management.

Early warning offers more time for analysis, planning and response planning, and in case of reaction, it increases the chances for an operation to be successful.

At the same time, ongoing development methodologies regarding information collection and analysis will have a vital importance when increasing the level of credibility and persuasion of the approach related to preventing conflicts (EW & ER).

The effectiveness of this process greatly depends upon its integration in the conflict prevention system and crises management, thus having a great importance for early warning. A solid basis for decision requires effective, rational and responsible combination of the two kinds of analysis methods (quantitative and qualitative), within the early warning systems of intelligence services.

Examples

1 ■ While a prospective attack threat with nuclear weapons will always have a great impact, the chances of such an attack to take place against a democratic country have decreased in the latest years.

2 ■ There are cases in which decisions-makers look suspiciously at the intelligence services warnings, which could however be valid. Obviously, in such cases, decision-makers must take into account the data collected from other resources as well, other than the ones provided by intelligence services, still, information offered by them must not be ignored when a certain strategy must appear.

2A ■ Previous to the Yom Kippur War, 1973, Secretary of State Henry Kissinger and the Israeli political leaders of that time did not take into account the intelligence services warnings regarding Egypt's war intentions. H. Kissinger looked with distrust at these warnings, maybe because they were not supporting the previous ideas, and, on the other hand, due to the fact that other intelligence structures assured him that Egypt and Syria's intentions are peaceful.

H. Kissinger was surprised when the Egyptian troops crossed the Suez Canal.

2B ■ Some Western intelligence services warned the political leaders about an upcoming Soviet invasion of Afghanistan in 1979. Nevertheless, some of them preferred to trust Leonid Brejnev, USSR President, who claimed that the invasion would not take place.

The heads of state and government who trusted President Leonid Brejnev's assurance were surprised when the Soviets entered Kabul.

In other cases, not reacting represents a way of action.

2C ■ Throughout the Second World War, British Prime Minister William Churchill received a warning about the bombing of the city of Coventry – lacking military importance – by the Germans. Notwithstanding, W. Churchill did not do anything and, as a follow-up to the bombings, there were a lot of victims and considerable damage. Had any kind of defence measure been taken, it would have revealed the British success in breaking the German communication codes (*Enigma*) and the existence of signals capacities developed by the UK. Churchill did not react in any way, thus protecting the strategic intelligence advantage.

The key element disappears when decisions-makers take into account the data from a warning.

2D ■ The best example in this respect is the one provided by the Romanian military intelligence service, which, in August 1968, properly informed the country leadership about a potential reoccurrence of the "*Czech pattern*" in Romania.

3 ■ During the Second World War, as a follow-up to a warning regarding the Japanese plans to invade Midway Island, Admiral Nimitz took the decision to attack advanced elements of Japanese fleet, although the information was incomplete. Following the decision, the Admiral was successful in destroying a part of the Japanese fleet.

4 ■ A tactical-operational threat could be that an enemy country launched an intercontinental missile. The time from launch until it reaches the target

is very short, limiting the decision choices of the military decision-makers in charge. The enemy is already “*at the gate*”, and the military decision-makers have to deal with the “*crisis management*”.

5 ■ The greatest failure of US intelligence services was the one regarding the Japanese attack on Pearl Harbour, in December 1941. The fleet commander from the Pacific, Admiral Husband Kimmel, received warning information from Washington while the attack was already happening.

Regarding the Pearl Harbour attack, there is also the opinion according to which the US had enough information about an upcoming Japanese attack, but actions were not taken in order to get the public opinion to agree with the US decision of starting war.

A supportive aspect in this respect was given by the fact that the Japanese Ambassador asked to be received by the US Secretary of State precisely at the time when the Japanese Air Force launched the attack. The purpose was to hand in the declaration of war. Knowing the purpose of the visit, the Secretary of State kept him waiting, without giving him the chance to communicate outside, receiving him after the beginning of the attack. Thus, Japan attacked the US without a declaration of war.

After the Japanese attack, Roosevelt called Churchill, telling him: “*They have attacked us at Pearl Harbour. We are all in the same boat now*”.

6 ■ It happened in October 1973, when the Egyptian troops, crossing the Suez Canal, headed towards the Israeli posts in Sinai, after several warnings associated with military exercises taking place in the area. When, in September, the Israeli intelligence services found out about Egyptian war plans, Israeli military leaders looked at them as “*another routine exercise carried out by the Egyptian Air Forces*”. Not even the fact that Soviet ships left Alexandria harbour just few days before the beginning of war determined the Israeli leaders to reconsider their attitude and react accordingly.

As mentioned above, in 1973, the Egyptian Army carried out several military exercises which reduced Israel concerns about a probable attack. The Chief of military intelligence service, General Eli Zeira, thought that Egypt would not go to war as long as Israel had air force superiority. This was one aspect from a series of mistakes made by Israel and recognised later on in a report entitled “*The Concept*”. The idea according to which Zeira lacked a strategic concept suitable for the situation spread fast. Within this framework, his judgment was influenced by the fear of not raising a false alarm, taking into account the fact that, in May 1973,

Israel spent approximately 10 million dollars for troop deployment, due to an Egyptian military exercise. Because nothing happened, the media and the government criticised the military leaders. General Zeira knew that a second deployment, in less than five months, due to an Egyptian exercise, would end his career. The Israeli intelligence services received, prior to October 1973, approximately 1 500 reports regarding the Egyptian plans of war, but General Zeira did not warn the decision-makers. The criticism and the expenses associated with a prior false alarm caused that state of mind among Israeli intelligence.

BIBLIOGRAPHY

1. A. Matveevna, *Early Warning and Early Response: Conceptual and Empirical Dilemmas*, European Centre for Conflict Prevention, 2006.
2. R. Ștefănescu, *Systems, Indicators and OSINT Platforms for Early Warning, Monitoring and Analysis* (Annual international session of science communications), 2009, București, vol. 1.



OPEN SOURCE INTELLIGENCE

– Opportunities to Support and Develop High-Performance and Effective Education System in the Defence Intelligence Field –

Colonel Dr Cristian-Victor CIȘMIGIU

OSINT and the Current Information Society

The Romanian military body transformation has required a new approach to education activities in line with the objective necessity to harmonise higher education and, by extension, specialised military higher education with the exigencies generated by the signature of the Bologna Declaration by our country in 1999.

In this complex context, the author considers that defence intelligence education, a field whose continued evolution has generated the need for complex and effective education services, has undergone a series of significant changes involving the education subject (student), the education support (documentary resource) and the education provider (professor/trainer).

Keywords: *education process; defence intelligence; information society; OSINT*

It is widely acknowledged that the information society is the society in which the production and consumption of information is the most important type of activity, information being recognised as the central resource, information and communication technologies being core technologies and information environment, together with the social one – a sine qua non environment of human existence.

The rapid development of information technology in the past years has had an increasing impact on society in general. A significant part of the premises of the transition to the information society was dictated by the growing social dynamics after 1990. In this context, digital technologies have gradually become more accessible and cheaper, enabling a growing number of users to access, process, store and send information.

Gradually, the exponentially increased volume of available information has generated,

Colonel Dr Cristian-Victor Cișmigiu – “General Nicolae Condeescu” Defence Intelligence Training School, București.

on the one hand, opportunities for exploitation by creating high performance products and services, developing new social activities and, on the other hand, it has facilitated the premises of the transition to information society by finding a part from its domains and features, the most significant of which being the social, economic and cultural ones.

The transition to modern, information society, against the background of a globalisation with an unprecedented momentum at the beginning of the third millennium and the crystallisation of freedom of expression and increasing interest in change and continuous development, has resulted, in all areas of social life, especially in the field of education, in a significant increase in the importance of open and widely accessible source information, its identification, analysis and use becoming an inseparable element of contemporary knowledge and development processes.

Currently, it is accepted the theory that *Open Source Data* (radio/TV shows, printed data, unprocessed signals, photographs, tapes, satellite images, personal letters) and *Open Source Information* (correlated and processed data for general interest information, media articles, books, communiqués) as complementary elements of a process meant to contribute to the foundation of *Open Source Intelligence (OSINT)*, provide between 80 and 95% of the data used by the intelligence community worldwide¹.

This complex process is aimed primarily at providing historical and cultural-strategic knowledge, operational information regarding infrastructure and social developments, commercial geospatial information vital from the tactical point of view, which cannot be obtained by other means.

Specialised literature pays high attention and analyses the field of *Open Source Intelligence* and highlights, in a nearly exhaustive manner, that this field involves the identification and validation of sources, collection, processing, analysis and exploitation of information for the development and dissemination of products with relevance in the field of national security, which meet the specific intelligence requirements.

In the same context, there are also specified the main categories of sources that contribute to this process, either classical (periodicals, documentaries, radio and television broadcasts, official data expressed by government reports, data and information from different professional and academic environments, geospatial data, gray literature etc.) or modern (interactive, digital media products, shared

¹At <http://www.sri.ro/categorii/56/centrul-surse-deschise.html>.

through computer networks or the totality of texts, sounds, images and graphics processed on the computer and collected in databases, “social media” of communication, collaboration, recommendation etc.).

Cognitive-Information Approach to the Education Process

One of the most recent ways of approaching the education process is the cognitive-information one. This type of approach more and more obviously shapes a new and sophisticated model of learning/training, the information-type one, determined by the new operational and conceptual framework, with deep roots in the theories of cognitivism and information processing.

Thus, an education system emerges in which information processing and communication become synergistic elements specific to an approach that exists “... around the concept of cognition seen as an activity of construction of individual knowledge through the processing of information and the products of this activity, namely the ensemble of constructed knowledge”².

The application of this system highlights the shift from the pedagogy of communication and action to the pedagogy of information transformation and processing in an institutionalised training framework, much influenced and determined by the presence of new sources of information and communication available to society today.

The new framework of education activity is under the impact of computerisation, the pupil/student/learner being continuously subjected to the bombing of certain stimuli containing a high load of data and information and which they are forced to face selectively.

Thus, according to cognitive science, the pupil/student/learner can be seen as a large plant for the reception, processing, storage and use of information. The information received subsequently turns, by processing, into elements that contribute to achieving competencies/performance at a cognitive, psycho-moral, psychomotor etc. level.

It can be said that to the “... reflective property of the psyche one adds an information feature, and mental processes, interpreted in cognitivist terms, are essentially information processes, which can be treated with the information apparatus derived from the concept of information...”³. In this way, information processing becomes indivisible part of any information system, including the education one.

² Ioan Cerghit, *Sisteme de instruire alternative și complementare – structuri, stiluri și strategii*, Editura Polirom, Iași, 2008, apud Fr. Raynal, Al. Rieunier, ESF, *Pédagogie: dictionnaire des concepts clés (apprentissage, formation et psychologie cognitive)*, Paris, 1997.

³ *Ibid* apud M. Zlate, *Psihologia mecanismelor cognitive*, Editura Polirom, Iași, 1999.

Being in a training situation, the pupil/student/learner obtains pieces of information in the institutionalised education environment under the form of certain stimuli from several types of sources, the teacher/trainer, courses, regulations, related teaching resources, training videos, internet etc. being just a few of the most important ones.

These pieces of information, which involve a various degree of processing and are parts of the information, cultural and socio-professional system, acquire scientific values for whose way of transmission/reception, complexity and validity of sent content is directly responsible the teacher/trainer – pupil/student/learner binomial.

In context, it follows that the information, seen in a teaching-education perspective, becomes an essential part of the education process and is the substance of training and education. This type of information, much different from the usual semantic information, meets a set of values that need to be considered permanently by the beneficiary of the teaching, to which they must especially relate when the teacher/trainer is eliminated from the cognition process and deliberately uses open source intelligence for their own training.

One can appreciate that one piece of information could have education elements provided that it is: rigorously selected and evaluated in keeping with scientifically determined value criteria, systemic, valid, contextualised, with limited redundancy etc. A careful analysis of these criteria is essential for a deeper understanding of the way in which the teaching information could be used effectively, pupils/students/learners will be able to process the information they get in contact with, and on this basis they will be able to create their own “*baggage*” of knowledge and actions.

OSINT for Effective and High-Performance Education in the Defence Intelligence Education

The evolutions of the security environment at the beginning of the third millennium, combined with unprecedented information explosion, have undoubtedly caused the need for knowledge, education and training in the whole society.

Therefore, it has become a fact that one can no longer speak of capacity for adaptation, progress, a new vision in every area of social life outside an acute and permanent need for information, in general, and for access to education information, especially when talking about scientific entities.

Against this background, distinct categories of recipients of information have emerged and developed, a special place belonging to the ones in the education

field, technologies and systems for processing them have been created and improved, the foundations of an information culture as a product of the information society have been laid. A permanent need for training has emerged in the sense of creating the skills to effectively identify, evaluate and use the information essential to achieve a particular purpose, requirement, responsibility etc.

This explains the fact that, gradually, the information society, by implementing new information and communication technologies, has created the opportunity for unprecedented flexibility in classical education, an aspect also generated by the increasing need for certain independence at the space-time level of the learning activity, which can be largely achieved through the broader use of open source intelligence.

From the utility of this category of sources can benefit both individuals and institutions in different fields of activity and study, more or less restrictive in terms of access to primary information, this latter indicator being generated by the degree to which the beneficiary of the information is connected to an activity which is in some degree of complementary to the field of national security.

Referring to the education in the field of defence intelligence, a process that is also undergoing transformation, one must highlight that more than ever in the history of Romanian military body, as well as of the intelligence structures of the military, now, the focus is on identifying the most suitable aspects aimed at continuously improving the elements that make up the framework in which the education takes place in that specific field: learning subject, support and initiator.

If, as far as the learning subject and initiator are concerned, a series of national and sector education and human resource policies have been designed and implemented, whose results will be probably outlined in the next 3-5 years, which is directly dependent on the current social-economic realities, the learning support, unfortunately, has not been given the necessary attention, being even placed in the background of the approach.

It is already known that, in its effort to pre-and post-accession to the Euro-Atlantic bodies, Romania, through its essential vector of providing national security, started and is currently carrying out an extensive process of operational and conceptual transformation, which could not take place without a thorough analysis, study and use, adapted to the Romanian realities, of all social, cultural, education and institutional sources that the above-mentioned bodies have made available in this respect.

Unfortunately, but only for now, not adapting some elements related to the legislation that governs the access to different kinds of information, especially

in the military field, in different branches related to it, as well as the persistence of certain mentalities and beliefs often artificially and exaggeratedly restrictive create a number of difficulties and make difficult the education, training and preparation process, in general. By extension, it is difficult for the entire education act, especially the one applied to areas under the responsibility of national security, to meet in a short time certain parameters compatible with those of the related activity systems and domains of the armed forces of NATO and the European Union member states.

That is why we think that it is required a careful and thorough analysis of the way in which the learning support in the field of defence intelligence should be improved as fast as possible. This requires will, entrepreneurial spirit, creativity, originality, vision and sustained intellectual capacity from the learning initiator and subject as well as the decision-makers, in order to interlock, in optimal conditions, strictly respecting legality, all specialised data and information obtained from traditional sources (instructions, regulations, rules, procedures etc.) with those made available through open source intelligence. This actually is one of the sure ways in which specialised education can really be reshaped and streamlined in the next period.

In this context, without claiming to be complete, we may highlight, based on experience and current education practice, from a strong pedagogical perspective, a series of elements (advantages-disadvantages) that we consider to be most significant to be considered when analysing the utility and opportunities offered by the use of open source intelligence in order to support, develop and improve education in the field of defence intelligence.

Thus, among the advantages that may be brought about by the use of open sources, one may mention:

- they provide data in a volume and quality that cannot be obtained from secret sources and enable the access to certain types of expertise that is not always accessible because of the lack of (time, material, financial etc.) resources;
- they implicitly lead to increasing possibilities of manifestation of imagination, creativity and resolute anticipations;
- they enable teachers/trainers to diversify education strategies, providing them, at the same time, with a socio-psycho-education database capable of optimising the teaching-learning-evaluation process;
- they generate the development of information processing strategies by expanding the consultation framework and a knowledge environment complementary to the personality of the pupil/student/learner;

- they provide optimal conditions to enable acquisition knowledge or expression of ideas in various ways and the elements that are minimally necessary for contextual understanding in the primary information analysis stage;
- they provide the pupil/student/learner with the possibility, depending on the domains of interests, of accessing databases to supplement the course, instructions, regulations data or even to establish contacts for clarifications or further collaborations with internal or external partners;
- they enable the pupil/student/learner to access information at their own pace of assimilation, to speed up or slow down learning, as well as to access alternative versions of interpretations of certain notions, terms, activities, specialised processes from an unclassified perspective of information;
- they enable all participants in the education process to adjust to the multiple styles of teaching-learning and provide a high degree of memorising the information;
- they provide the pupil/student/learned with the possibility of choosing the content and methods corresponding to different interests, needs and levels of ability/skills to be reached;
- they enable the exploitation and capitalisation, in optimal space and time conditions, of all opportunities and possibilities of using a broad as possible range of written resources (handbooks, courses, classical didactical materials), audiovisual messages, images, graphs and interactive video techniques, animation, cable broadcasts, simulations, computer-assisted training, CD-ROMs;
- depending on the type and support of information, they make possible the development of a specialised vocabulary, technical, information, analytical and linguistic skills of users;
- they make available communication and information resources, in support of teachers/trainers and pupils/students/learners, with a high teaching and learning potential.

Among the disadvantages of the implementation of the infrastructure needed for using open source intelligence and the use of this kind of intelligence itself, one may mention:

- high costs for its establishment and, consequently, for permanently adapting to continuously evolving standards;
- substantial costs regarding the quality, quantity and verity of the information that is accessed;
- modernisation of information access and transfer routes requires the periodical specialised training of users, both at home and abroad;

- it may cause difficulties when organising the study and managing the time necessary for it in the absence of methodical specialised instructions etc.;
- use of variable information sources without setting clear objectives favours a high degree of information redundancy and may even lead to altering the perception of the real world;
- unlimited use may cause an acute state of isolation of the beneficiary with socio-psychological implications that are difficult to assess;
- use of open source intelligence in sensitive domains such as national security without a proper specialised training may subject the user to information manipulation through intoxication, persuasion and disinformation, with consequences difficult to assess and eliminate subsequently;
- use of open sources without prior proper training brings about an information overload that is difficult to manage by users.

*

The use of open source intelligence may have direct and immediate consequences for the quality of defence intelligence education, being a real instrument for streamlining professional training, specialisation, professional reorientation, updating the knowledge and continuous training.

That is why pupils/students/learners, teachers/trainers, as well as decision-makers in this domain must be aware of this need and make intensified and determined efforts to remove, as much and as fast as possible, the conceptual and operational legal barriers that are present, as we have previously shown.


Among the solutions we deem necessary to be considered and materialised with the purpose of obtaining an efficient and high performance education in the field of defence intelligence, by expanding the use of open source intelligence, we mention:

- to create an IT infrastructure to meet the international standards in the field, capable of exploiting with increased efficiency open source intelligence;
- to harmonise the design, planning, organisation and development efforts, at the level of the most important institutions in the field of defence intelligence, for a complex programme of training in the field of exploiting open source intelligence for the teachers/trainers involved in the mentioned field;
- to establish, within the defence intelligence education structures, specialised structures for information-documentation that must efficiently contribute to qualitatively managing open source intelligence and to educating users in this respect;

- to start teaching, within the education curricula related to defence intelligence, the course “*Analysis, evaluation and use of open source intelligence in the field of defence intelligence*” for each education level: bachelor’s degree, master’s degree, continuous training through career and level courses, graduate and doctoral studies;
- to create and develop long distance and low frequency learning for various training forms in the field of defence intelligence.

BIBLIOGRAPHY

1. P. Atanasiu, *Metode și tehnici de lucru pentru sisteme de informare științifică*, Editura Didactică și Pedagogică, București, 1976.
2. D. Banciu, *Sisteme automatizate de informare și documentare*, Editura Tehnică, București, 1997.
3. M. Brut, *Instrumente pentru e-Learning. Ghid informatic al profesorului modern*, Editura Polirom, Iași, 2006.
4. Ș. Buzărnescu, *Sociologia opiniei publice*, Editura Didactică și Pedagogică, București, 2000.
5. L.E. Danciu, *Educația deschisă și la distanță*, Editura Eurostampa, Timișoara, 2002.
6. A. Mucchielli, *Tehnici de manipulare*, Editura Polirom, Iași, 2002.
7. I. Stoica, *Structuri și relații informaționale în dezvoltarea învățământului și a cercetării românești*, Editura Alternative, București, 1997.
8. C. Zamfir (coord.), *Dicționar de sociologie*, Editura Babel, București, 1998.

English version by
 **Iulia NĂSTASIE**

AIRPOWER IN THE ASYMMETRICAL CONFLICT

Case Study: Afghanistan (II)

Major General (AF) Dr Victor STRÎMBEANU

ISR capabilities are transforming, the air situation visualisation is almost permanent and it has decentralised up to sub-tactical levels. The time for delivering close air support has shortened, by the dynamical allocation of targets, to periods difficult to imagine in the past. At the same time, the quality and precision of close air support have evolved up to providing the capability of distinguishing between individuals. On the other hand, airforce robotisation has been assuming more and more classical missions of the vehicles with human crew onboard, from research, electronic warfare to combat missions and airlift. Robotisation is only at the beginning, the author considers, and the future will definitely witness an explosion of the unmanned air vehicles, especially in the high risk areas.

Keywords: *air transport; forces extraction; asymmetrical conflict; robotisation; Afghanistan*

Robotisation

In Western democracies, the public opinion, expressed in various ways, but, in the last resort, by vote, is sensitive to human losses in conflicts far from the national territory, which are not perceived as a direct, immediate threat. Raising public awareness is directly proportional to the reflection of those losses in the media, which is in a directly proportional relation to the exponential technological progress. In their turn, the policymakers in democracies, even if they are not directly concerned with the human losses in the armed conflicts they manage, are dependent upon the public opinion, especially upon its electoral expression and consequently they act in all the directions that are likely to stimulate a favourable electorate, including in the sense of limiting human losses in armed conflicts. Therefore, they are likely to spend significant resources to provide the technological progress meant

to increase combat actions efficiency, limit own human casualties or even replace the human resource in risk area, wherever possible, even if this requires major expenses. The impact of human losses on the public opinion is bigger than the effect of certain consistent defence budgets.

Major General (AF) Dr Victor Strîmbeanu – Chief of Training and Doctrine, the Romanian Air Force Staff, the Ministry of National Defence.

As far as airpower in asymmetrical conflicts is concerned, this phenomenon is reflected most visibly in the tendency to replace human crews onboard the aircraft with flying robots, with sophisticated “*drones*”, which undertake more and more the traditional missions of human pilots, navigators, shooters, air observers etc. In the first part of the article, we already wrote about the use of *UAVs* in aerial reconnaissance missions. We are basically witnessing a technical boom of unmanned aerial reconnaissance means, at all levels, from strategic to micro-tactical. And the real change we are witnessing takes place at this latter level (sub-tactical, micro-tactical). If, at strategic level, the issue of aerial reconnaissance was settled quite a while ago, at micro-tactical level, a mini-revolution in military actions is taking place just now, by diversifying the means for aerial reconnaissance, the small and extra small dimension ones, with fixed or rotating wings, which are now part of the equipment of the companies, platoons and even groups of infantry, special forces, simple, easy aerial means, which can be operated immediately, with minimum training, by one or two operators at most and which, once launched, send vital information in real time from the area of interest of the respective group or platoon. As mentioned above, the diversification and extent of aerial reconnaissance at micro-tactical level have already brought about changes in information management and in the decision-making process. Actually, it is difficult to argue if this phenomenon is still connected to airpower per se or it is just a reflection of applying airpower with a catalytic and effort multiplying effect on land forces.

Another significant aspect of robotisation is the significant technological step from *UAV* to *UCAV*, from simple unmanned aerial vehicles, mostly used for aerial reconnaissance, surveillance, to unmanned **combat** aerial vehicles. It is a radical progress in airpower, being still in an incipient phase, whose final effect cannot be assessed yet. One may still conclude that this step, from *UAV* to *UCAV*, will radically change the air forces, the way of applying airpower and the warfare, in the last resort. Lately, in Afghanistan, *UCAVs* have been used more and more and with better and better results. They are less expensive than manned combat aircraft, less dependent on human errors and vulnerabilities, smaller, with reduced radar and infrared signatures, *stealth* elements, high capacity of survival in the tactical field, in other words, the probability of being taken down by the enemy forces, as far as they are concerned, is low. In fact, in the confrontation with “*drones*”, the stress is not laid on taking them down, but rather on jamming them and, eventually, taking control over them, which represents the new opening in the evolution of aerial warfare and, at the same time, the supreme victory in this particular aspect of armed confrontation, because a “*drone*” that is intercepted and taken over can be used, as a last resort, against the forces it belongs to.

The “*unmanned*” feature of these aircraft must be understood as being “*without crew on board*”, and not as “*unpiloted*”. In reality, they are extremely well piloted, but from a distance, which, irrespective of the level of protection, encoding, redundancy, makes them vulnerable to jamming and, implicitly, the control over them can be lost, they can crash or even be taken over by enemy forces. The warfare of the future will witness the confrontation for, on the one hand, keeping control of own “*drones*” and, on the other hand, blocking and taking control of enemy drones. Obviously, insurgent forces cannot have access to such technologies, during this stage. One cannot say the same about certain states, which, for various reasons, sympathise with and support the insurgency, in general, and the Afghan one, in particular.

It is not impossible, just as in the past, during the anti-Soviet war, for insurgent forces to receive assistance in technology and specialists from states possessing such capabilities, able to employ robotic forces of the coalition. The loss of a “*drone*”, in October 2011, in a neighbouring country of Afghanistan, which was declared “*crashed*” by the allied forces and claimed to be “*shot down*” by enemy forces, was trumpeted as a great victory against the coalition. Judging by the nearly intact drone “*crashed*”, it may be presumed that one gained access to its command-control system and finally redirected the aircraft to another destination.

However, the conclusion is obvious and certain. The robotisation of aerial means has made significant progress. In Afghanistan, the drones are currently undertaking an important part of traditional air force missions (reconnaissance, surveillance, electronic warfare, ground attack, close air support etc.). More recently, there have been tested and applied the loading/unloading of containers using robot (unmanned) helicopters and the transport of logistics (ammunition, supplies) by air in high-risk areas. In fact, these attempts are not so new. They started years ago, by the testing of cargo gliders. However, they had a number of disadvantages, due to the fixed wing and the lack of a propulsion system, thus seriously limiting the freedom of movement. Then, the next step was taken towards rotary wings (helicopters). In Afghanistan, US Marines successfully tested the *K-MAX* system [a robot helicopter with two rotors, able to lift a payload of 3,5 tonnes and to transport it at 250 miles (about 400 km), and this was not the first robot helicopter used by the Marines (it was preceded, for example, by the Boeing product “*A 160 Hummingbird*”, a smaller and less powerful version)]. The *K-MAX* system proved to be so efficient that one began to exploit it, initially for six months, a further decision extending its use to 2013 or more. Therefore, robotisation undertakes more and more “*classic*” missions of airpower.

Airlift

In a theatre of operations such as Afghanistan, which is large (over 1 000 000 km²), with high altitudes, difficult to reach, intra-theatre airlift is essential for both troops and the necessary resources to support operations. Intra-theatre airlift is carried out with a broad range of medium-sized military transport aircraft, of the allies and partners, Afghans included, the most used being C-130, C-160, An-12, C-27, An-72, An-32 and with heavy lift helicopters (CH-47, UH-60, Mi-17, Mi-8, Puma etc.). Some types of helicopters have gone through special modernisation programmes with a view to being used in Afghanistan, such as increasing the power of engines in order to make them operable at the extreme heights and temperatures in Afghanistan, protecting against erosion caused by sand (special filters for engines, treating the blades of impellers and anti-torque propellers), reinforcements, armours, anti-crash seats etc.

Extra-theatre airlift is even more important than the intra-theatre one. Thousands of kilometres away from the troops and supply contributing countries, with neighbours that are rather unfavourable to the coalition, which allow the transit of their territory and airspace with difficulty, most frequently based on agreements that are intensely supported financially by the international coalition, the airlift necessary for maintaining the effort in Afghanistan is vital. As the rotation of contingents consists of more than one hundred thousand people, the resources necessary for supporting them and the tempo of operations (fuel, food, ammunitions) are a significant effort, which is mostly supported by air. For this there are used especially big aircraft, so-called “strategic” (B-747, C-5 “Galaxy”, An-124, A-300, Lockheed L-1011 Tristar) contracted or belonging to allied air forces, and inter-classes (C-17, IL-76) or medium-sized transport (C-17, C-130, C-160) ones, even if the latter ones must stop to refuel in allied or partner countries. Given the long distance from the resources, it was required the establishment of an air bridgehead (Manas), in a partner country (Turkmenistan), in the proximity of the theatre of operations, which should activate as a super-APOD/APOE (*Airport of Disembarkation/Embarkation*), in fact, a kind of staging area for troops, materials, fuel, food, water.

In order to facilitate the operation, operational commanders do not measure the logistic resources in conventional units (tonnes, litres, kilograms), but in *Days of Supplies (for Operations) – DOS*, established in current, normal, attention, critical etc. values/thresholds. Any day a APOD is closed (because of insurgent attacks or bad weather, sand storms, heavy snowfalls etc.) is immediately reflected in the decrease in the number of days of supply, and, even more, in the reduction of the tempo of operations, measures to cut consumption, identification of alternative supply solutions. For instance, the closing of Pakistan borders, after the accidental

killing of 24 Pakistani soldiers at the “*Salala*” border post (NNW Peshawar), in a close air support mission, on 26 November 2011, caused extra and difficult-to-manage stress, on the main NATO *APODs* (Kabul, Kandahar) and on the other ones, led by certain allied nations (Herat, Mazar-e-Sharif, Bagram, Bastion), which worked anyway 24/7 in difficult circumstances.

CSAR, MEDEVAC, CASEVAC

The missions mentioned in the acronyms in this subtitle are carried out continuously in Afghanistan on a daily basis, either they refer to *Combat Search and Rescue – CSAR*, *Medical Evacuation – MEDEVAC* or *Casualty Evacuation – CASEVAC*. *Role 1, 2 or 3*-type medical formations work 24/7. When they are not at full capacity, they are used for Afghan civilian patients, including children, this being one of the most efficient forms of influence. After patients are stabilised, if the level of complexity of surgical interventions is above *Role 3*, the patients are evacuated as emergencies, obviously by air, to superior-level hospitals, in Germany.

Both *CSAR* forces and means (helicopters) and *MEDEVAC* ones usually work as *Quick Reaction Force – QRF*. As we have already mentioned, even if they follow the rule of the patrol flight, in order to support each other in case of attack, followed or not by forces landings in unknown territory (basically, in conflicts of this type, the entire territory is considered enemy territory). In this case, as, in fact, in all the fields and throughout the asymmetrical conflict, a continuous “*tactical dialogue*” takes place between belligerents, based on which each party adapts its tactics. For instance, insurgents have learned very fast that, after each person they wound among allied forces patrols, a support or medical evacuation helicopter appears. And they have begun to organise their forces to attack it, shooting down a helicopter being much more spectacular and having a greater impact than a few wounded persons on the ground. The allied forces have imposed immediately the rule of patrol flight for helicopters, so that, while one of them takes care of the extraction per se of the wounded persons, the other ensures it and supports it from the air. To quickly identify the landing site it was required that those who asked for air support should mark it by day with red smoke grenades and by night with light signals or stroboscope. The insurgents also noticed those signals and began to “*mark*” their landing sites, with red smoke grenades or lights similar to those used by the allies in order to ambush those helicopters, where insurgent forces were waiting with proper weapons for shooting down helicopters. “*Marking*” the landing site by insurgents takes place in a coordinated manner, when the helicopter gets near, because the smoke persists only for a few minutes, as logic as possible,

at places close to the *TIC* event, in order for the action to seem credible, but far enough from it not to make the engagement of the forces that demanded air support possible (600-800 m at 1,5-2 km). Allied forces then changed the colour code of smoke and light signals, on hours or periods, so that, if the colour of the smoke or the signal used for that particular moment did not correspond to the ones previously set, it should not be taken into account, thus avoiding the ambush. There were many cases in which allied helicopter crews were misled in this way.

The Case of LASER Lights

Directly related to the attacks on air means, in order to increase their efficiency, insurgents develop and maintain their shooting skills by practicing, without opening fire, on aircraft landing or taking off, day and night, from the big *APODs*. Very frequently, crews reported laser light situations, especially during landing. After investigating the situations reported, accidental illumination by own forces or by children with laser toys was excluded. Lighting is made with professional means, from much greater distances than commercial means can reach, but within the efficiency range of the portable surface-to-air weapons. In fact, special orders were sent to all allied and Afghan bases in the areas of occurrence of these phenomena not to use laser equipment on military or civilian aircraft landing on or taking off from those *APODs*. The crew's response to the emergence of these laser lights is, logically, to carry out defensive manoeuvres, anti-missile ones, of missing the landing and repeating the procedure, possibly differently, if the situation allows it. Sometimes, especially in the case of combat aircraft that still have ammunition on board when returning from mission, offensive manoeuvres are initiated, trying to identify the precise source of the light in order to attack it, which is extremely difficult in urban areas, given the circumstances in which collateral damage must be avoided. The crew's response is logical, of self-defence, because one cannot know when that laser light is for "*training*" and when for a real strike. Allied forces, in cooperation with the Afghan government ones, tried to establish the sources and capture the authors, but without success, since, even when using *ISR* means, the short duration (seconds) of the laser lights in these urban areas made it impossible for the persons behind these actions to be identified and caught.

Predictability and its Risks

The "*tactical dialogue*" is continuous and whoever ceases to permanently adapt immediately pays the price. A basic rule in asymmetrical conflicts, which can be applied to some extent in other types of conflicts, for air and land forces as well, is to *avoid predictability*. And allied forces, acting based on well-established SOPs,

were very vulnerable in this regard. One of the first consequences of this predictability to the detriment of allied forces resulted in the tactic of insurgents of detonating a small *IED*, with minor effects, on some individuals, then waiting for intervention forces, which came with mathematical certainty, on the ground or by air, and on which they would detonate a much powerful *IED*, previously located nearby precisely for this purpose. The adaptation came under the form of the more or less random change of the standards of intervention, of the reconnaissance of the area before the intervention of support forces, although it sometimes involves delays that could worsen the situation of the wounded.

Repeating the same trajectories, at the same heights and speeds, again exposes the allied air forces and means to insurgent attacks. Some of these elements can be changed routinely to prevent attacks, but other procedures, such as the landing and take-off, cannot be changed or cannot be changed enough to get a noticeable effect, because take-off-landing runways and platforms cannot be moved, and the aircraft, regardless of the defensive developments adopted, should finally reach the point of contact (*touch-down*) after a more or less standard slope. In these circumstances, the only viable solution left for allied forces was to take control of adjacent areas, parts of larger areas of ground defence (*“Ground Defence Area”*) with enhanced control on take-off-landing directions, where aircraft are more vulnerable, since landing procedures involve flights at low speed and height, with limited room for manoeuvre because of small energy reserves. This control requires constant surveillance by *ISR* means, permanent patrolling for observation, monitoring, deterrence, show of force, cooperation with local authorities to monitor the population in the area and possible insurgent infiltration. Even so, the vulnerability remains and there is no guarantee of safety. Wherever possible, crews adopt special procedures for landing (they get closer at greater heights and increase the rate of descent on the landing track) to reduce exposure time. The interference of states with air-to-surface capabilities and easier access to portable guided surface-to-air weapons for insurgents would be catastrophic for the allied air forces in theatre of operations. The experience of the Soviet war in Afghanistan confirms this, one of the decisive factors of the Soviet defeat being the large number (over 300) of helicopters shot down by insurgents using *“Stinger”* missiles and professional assistance.

“Repeaters” Campaign

Another sequence of the *“tactical dialogue”* previously mentioned is the competition for developing and maintaining a communication system by insurgents, concomitantly with the coalition’s efforts to disable it. This competition has several components, of which intercepting insurgent calls made from public fixed

and mobile telephone networks, monitoring them and exploiting information gathered are not the less important ones. The response from insurgents to this sequence of *“tactical dialogue”* was to develop an improvised, simple, but ingenious and functional communication system. Given, on the one hand, the predominantly mountainous terrain of Afghanistan and, on the other hand, the mostly sunny weather, the insurgents realised that they could use those features for their benefit, by locating, at high altitudes, a network of simple radio stations, each acting as a *“repeater”*, powered by a motorcycle battery almost continuously charged by a small solar panel attached, all of which being easily purchased on the open market. They managed in this way to build their own simple, inexpensive, easy-to-maintain communication system, through which they could communicate unlimitedly to coordinate their actions. The leading role in identifying and destroying the elements of this system belonged to the Air Force, this being another specific example of airpower in the asymmetrical conflict and, at the same time, the reason for approaching it in this context. If the station itself and the related antenna were difficult to detect visually, the solar panel, however, could be neither hidden nor camouflaged, being, by its nature, exposed to the sun. Most of the time, a 360° turn around the estimated position (by intercepting the electromagnetic emission source) was enough to *“catch”* a reflection of the sun produced by that solar panel, having a mirror role in this case, to identify the repeater and disable it. Given its simplicity, the repeater could be replicated and replaced relatively quickly after it was disabled by the allied forces, but after the aircraft crews assignments became experimented in this type of missions and received appropriate allocation of resources, restoring the network of repeaters became inefficient for insurgents.

High Value Targets ***– The Osama Bin Laden Case***

Another feature of the application of airpower in the asymmetrical conflict is hunting *“High Value Targets”* down. This category includes high-level insurgent leaders. They are followed in advance, using all forms of intelligence (*HUMINT*, *SIGINT*, *ELINT* etc.), including aerial reconnaissance, which requires a special effort, but is feasible and justified. Eliminating important leaders has highly beneficial effects for countering insurgency. The favourable occasions for neutralising them, without collateral or at least with limited damage, are rare events, which must be capitalised on immediately. For this, again, manned or unmanned aerial means are in the best position to act quickly and efficiently. Thus, either by permanently having force packages able to intervene in the shortest time or by *“dynamic targeting”*,

one ensures the capitalisation on these windows of opportunity in the most efficient way.

The special case of the neutralisation of the supreme leader of al-Qaeda, Osama bin Laden, although relevant, is not the best example, because in this situation, a sustained effort was required, over a period of several years, of careful planning and perfect execution, given that it was necessary to enter the airspace and territory of another state, with two manned helicopters and special forces.

Command-Control

Allied forces command in Afghanistan is performed by the Staff of ISAF (*International Security Assistance Force HQ*), through IJC (*ISAF Joint Command*) and the staffs of regional commanders (*Regional Commands, RC North, RC South, RC West, RC East, RC South-West and RC Capital*), also called “*Battle Space Owners*” – BSO. In the theatre of operations in Afghanistan there are eight BSO (6 regional commanders and 2 airport commanders, Kabul and Kandahar), who have one important ground defence area – *GDA*. IJC has a relatively short history. It was established in 2009, by separation from *ISAF HQ*, the latter still having responsibilities regarding the political and strategic management of the asymmetrical conflict in Afghanistan, while the *ICJ* was made in charge of the actual operational control, being responsible for implementing strategic directives, including through airpower. This is achieved through the *Combined Air Operation Centre – CAOC*, under the *IJC*, but outside the theatre of operations. Basically all air operations, including *AWACS* support, are led directly by this *CAOC*. Operational planning is managed at the level of *IJC*, through a specialised structure, headed by *Deputy Chief of Staff for Air Operations – DCOS AIR*, with visibility including over the Afghan Air Force, then implemented through the *CAOC* and carried out in a dynamic, flexible and decentralised manner to the level of crews or unmanned aircraft by the air forces of the international coalition.

*

Air power in the asymmetrical conflict deals with a paradox that apparently takes it out of its field of excellence, but, as part of a metaphorically conceptualised process – tactical dialogue – determines it in fact to adapt and develop new values without which the war against insurgency, disguised or integrated in the local population, would be infinitely more difficult to wage. ISR capabilities are transforming, the air situation visualisation is almost permanent and it has decentralised up to sub-tactical levels. The time for delivering close air support has shortened, by the dynamical allocation of targets, to periods difficult to imagine in the past.

At the same time, the quality and precision of close air support have evolved up to providing the capability of distinguishing between individuals. Yet, this does not completely rule out the risk of fratricide, as noted on several occasions. On the other hand, air force robotisation has been assuming more and more classical missions of vehicles with human crew onboard, from research, electronic warfare to combat missions and airlift. Robotisation is only at the beginning but the prospects are favourable and the future will definitely witness an explosion of the unmanned air vehicles, especially in high-risk areas. Intra- and extra-theatre airlift are vital for the insertion and extraction of forces, their rotation, the maintenance and support of operations specific to the asymmetrical conflict.

Without claiming the leading role, airpower has a vital, *sine qua non* role. It is, in fact, a further confirmation that any conflict, including the asymmetrical one, necessarily and compulsorily requires a joint effort.

Selective Bibliography

1. *Air Force Magazine* archives.
2. *Defense News* archives, 2011-2012.
3. *IHS Jane's Defense Weekly*.
4. *ISAF SAR Overnighter*, 2011-2012.
5. *Stars and Stripes*, 2011-2012.

English version by
✍️ *Iulia NĂSTASIE*

PSYCHOLOGICAL SELECTION TO JOIN THE MILITARY SYSTEM IN THE LIGHT OF THE MODEL OF MULTIPLE INTELLIGENCES

Colonel Dr Adrian PRISĂCARU

The model of the “theory of multiple intelligences” seems to be superior, from some standpoints, to the traditional model and it could provide conceptual or practical solutions not only to the vocational orientation but also to the psychological selection.

The classification of people according to their IQ, specific to the traditional model, is still valid and used by many practitioners. However, the pluralistic view on intelligence gets more and more followers. The new model accepts the fact that people have different cognitive powers and styles, which are specific to broad areas of human activity, and that their particular combination provides people with individuality.

Keywords: *candidates; aptitudes; military organisation; verbal intelligence*

Measure and measurement in psychology

In an outstanding treatise on the “*history and science of measurement*”, A. Robinson appreciates that “*man and measurement do not always go well together*”¹. However, the measurement of human nature, cognitive processes, body, and social events has developed from one decade to another.

Compared to the measurement of the concrete phenomena in the physical world, when it comes to the human being, the moral component is also important as well as some principles of causality pertaining to education, development, identity, and image. All these vectors affect or influence the precision and accuracy of measurements².

Although today, using the newest scientific achievement – the Nuclear Magnetic Resonance

Colonel psychologist Dr Adrian Prisăcaru – Head of the Psychology Laboratory of the Romanian Armed Forces General Staff, Associate Researcher, the Institute of Psychology of the Romanian Academy. The study was conducted by a team consisting of Colonel Psychologist Dr Adrian Prisăcaru, Colonel Psychologist Dr Gheorghe Chițu, Colonel Psychologist Dr Leonard Voloșin, Captain Psychologist Manuela Năstase, Psychologist Dr Lucia Iorga, Senior Psychologist Aurelian Mușat and Psychologist Dr Ana Maria Georgescu, within the Psychology Laboratory of the General Staff, the Ministry of National Defence.

¹ A. Robinson, *Măsura lucrurilor*, Editura Art, București, 2000.

² G. Nicola, A. Prisăcaru, *Măsura în știință și în istoria psihologiei*, București, 2009.

(NMR) technique –, we can see very clearly the structure of brain, tissues and cells, the mental processes that emerge in the challenging contexts of social life still remain unobserved. In other words, we have concrete investigative elements with regard to the neurophysiologic substratum, but this is only one of the conditions for the normal operation of the psyche, and the psyche and the processes that mediate the subject-object transaction still depend on subjectivism.

The concepts of “social life”, “problem solving”, “coping”, “civilisation”, “culture”, “set”, “cognitive intuition”, “automatism”, “stupidity” provide intelligence with architecture, it thus being the temple where all the situations meant for networking and social, organisational, professional and familial adaptation are officiated in the language of life and, more recently, in artificial forms³.

Therefore, it can be appreciated that intelligence, as a psychical dimension, represents a relation to the real, taking into consideration, more or less explicit, the structure of the problematic situation, and that it has implications for all life situations.

Some authors, trying to find an explanation and a concrete form to measure intelligence, by *Stanford-Binet test* and its variants, have classified people having different professions, age, activities, using a surprisingly general mathematical formula. Statistically defined performance, for a representative population, is related to the biological age of the concrete person, and in order to avoid the decimal number, it is multiplied by 100.

General intelligence (“g”), according to Spearman, or the “IQ”, according to Terman, has been subjected to reliability and validity tests, monitoring longitudinally typical lots of people and thus giving priority to experience, motivation and personal values. Intelligence measurement is acknowledged by recognising professional “merits”, by citing, accepting and assessing impact.

Given the psychic high functional mobility, potential and performance tests, as well as personality ones indicate a tendency of proximal development, leaving life to have the role of modelling forms, content, rhythms and meanings.

Measurement in psychology has notably expanded to other functions starting from sensitivity to the personality traits having emerging value such as emotional intelligence, problem solving related to the meaning of life etc.

It is appreciated that psychology has no methodological weaknesses in relation to natural science. Assigning a number to certain behaviour requires fairness and the condition of uniqueness of meanings. The fact that psychology uses primary measurements, such as brain waves or sensory thresholds (as in the case

³ *Ibidem.*

of intelligence or originality) is not a weakness of psychology. In all spheres of determinism, physical, chemical, astronomical, geological, biological, the two types of measurement are used. To be correct and unambiguous, other types of measurement are employed, starting with the significance of correlations.

If we analyse the current orientations of psychological practice we will notice the concern for formalisation, standardisation and unitary practice, both in psychometrics and psychotherapy, as a result of the need to harmonise and respond to measuring the effectiveness of psychological practice in the two mentioned sub-domains, namely behaviour prognosis and mental impairments or disorders correction.

In conclusion, the approach to measuring mental processes remains open to study. There is also a concern for developing the related methods, techniques and procedures, as well as the way obtained results are interpreted and exploited.

Theoretical models related to intelligence approach

Intelligence study has been a long-standing and constant concern and thus many theoretical orientations have appeared, addressing not only the extremely complex psychical process but also the design and operationalisation of assessment tools.

In specialised literature, the most common theoretical approaches are aimed at: the *psychometric model*, the *factorial model*, the *genetic model*, the *ecological model* and the *triarchic model*⁴. However, more recently, at the beginning of the '80s, to complement the above-mentioned traditional models, a new and interesting approach emerged, namely the "*theory of multiple intelligences*", presented by its author, Howard Gardner⁵, as an alternative model, guided by a new orientation regarding intelligence development and measurement, being, in essence, a pluralistic view. The model acknowledges many facets of intelligence and accepts the fact that people have different cognitive powers and styles, as well as distinct abilities, from musical intelligence to that involved in self-understanding.

The theory of multiple intelligences pluralises the traditional concept of intelligence, arguing that intelligence is a "*computational ability*", namely the ability to process a particular type of information or the ability to solve a particular type of problems based on certain operations or a set of identifiable operations⁶. It is estimated that each type of intelligence is activated or triggered

⁴ A. Andrieș, *Testarea psihologică. Aptitudini și inteligență*, Editura Fundația România de Măine, București, 2007.

⁵ H. Gardner, *Inteligențe multiple*, Editura Sigma, București, 2006.

⁶ *Ibidem*.

by certain types of information that are present internally or externally. The author concludes as follows: *“the theory of multiple intelligences better describes the human cognitive competence in terms of a set of abilities, talents or mental skills, called intelligences, and all normal individuals possess each of these skills to some extent, and the difference between them is given by the ratio of skills and the nature of their combination”*.

At first glance, we can say that the *“theory of multiple intelligences”* model seems to be superior, from some standpoints, to the traditional model and it may propose conceptual or practical solutions for psychological selection and vocational guidance.

The classification of people according to their IQ, specific to the traditional model, is still valid and used by many practitioners. However, the pluralistic view on intelligence gets more and more followers.

IQ measurement, approached as a one-dimensional view to assess intelligence, places people into two categories, some above the threshold/limit, namely allowed to attend a particular programme, and others below the threshold/limit, namely refused to attend the programme, perhaps for a single-point difference.

Undoubtedly, this approach works well for some people, the best and brightest being placed where they deserve to be, while those who are around the passing/failure threshold/limit area feeling certainly frustrated.

The one-dimensional view seems to be correct, as every person is treated equally and the measurement system is rational.

However, in the selection practice, there have been observations as well as some perplexities, such as: *“athletes with outstanding results, graduates of different institutions and different specialties with honours, specialists with expertise in different areas etc.”* sometimes get scores to the limit of admitted standard, though, undoubtedly, they have a certain intelligence that allows them to perform tasks related to learning or doing their jobs.

Therefore, a team of seven experts, having the goal of designing psychological tests following the *“theory of multiple intelligences”* model to develop the *“Methodology for the psychological selection of candidates for higher military education, post-secondary military education, and/or education/training programmes within the zonal selection and orientation centres”*, has designed a study on some aspects of multiple intelligence, presented in the following pages.

Hence, it may be inferred that, in the traditional manner or the one-dimensional view related to measuring intelligence, domains and large areas of human activity are not taken into consideration and that, in some cases, the examination/tests are not the most suitable or appropriate to the type of task they are meant for.

Based on these considerations as well as on some feedback that a facet of intelligence can develop only on the basis of other information processing

capabilities (facets) and it is fluently operable when several specific computational capabilities are present⁷, we have chosen to study the selection to join the military organisation in the light of the facets of multiple intelligences.

For each facet/type of intelligence our intention is that we should develop and use at least one test with a thematic content that is similar and specific to cognitive ability, and the evaluated persons should be required to solve similar problems throughout the test, which can help them to use their own reasoning and problem solving skills.

The choice/design of formal tests/examination used in the assessment/selection process related to the facets of intelligence represents an important milestone in the effort to validate the model. Tests can be an ally of specialists to recognise different cognitive characteristics, but only if they are designed to highlight rather than mask such differences.

Moreover, another important dimension of the study aims at capitalising on the obtained individual results and shaping the aptitude profile able to meet the requirement of vocational counselling/orientation, by emphasising and highlighting the specialties in which the person can achieve high efficiency.

Research methodology

The study on developing a *battery of psychological tests* to assess the facets of intelligence stems from the necessity to select candidates based on their skills in solving concrete tasks, at the performance standards required by the military organisation.

To achieve this goal, we established the necessary steps to develop the battery of tests, steps that ultimately materialised in *practical and applied objectives*, as follows:

O1 – to identify the most important facets of intelligence involved in military activity (phase I of research – expert method);

O2 – to define and operationalise concepts/intelligence facets (phase II of research – expert method);

O3 – to develop items for each facet of intelligence (phase III of research – expert method);

O4 – to design the *battery of psychological tests*, to implement them and to study the reliability and validity criteria (phase IV of research – experimental methods);

O5 – to finalise the form of the *battery of tests* and to establish the optimum psychological and aptitude profile (phase V of research – combined methods).

To achieve the first objective (to identify the most important facets of intelligence involved in the activity concerned), we operated with the “*theory of multiple intelligences*”

⁷ *Ibidem.*

model, developed by Gardner, and the profession-grams of military branches and specialties.

Using the method of experts (psychologists with expertise in psychological selection in the armed forces) in the identification of the most important facets of intelligence responsible for achieving performance in work, resulted six facets of intelligence, called “*specific facets*”, as follows:

- *verbal intelligence (V.I.);*
- *numerical intelligence (N.I.);*
- *spatial intelligence (S.I.);*
- *organisational and bureaucratic intelligence (O.B.I.);*
- *technical intelligence (T.I.);*
- *general learning intelligence (G.L.I.).*

In the second phase of research, aimed at defining and operationalising concepts/facets of intelligence (*O2*), each facet was defined, concepts were operationalised (the 6 facets of intelligence) and the importance of their assessment for the activities conducted in the workplace was established.

Mention should be made that the fundamental difference between the traditional model and the one of the theory of multiple intelligences with regard to assessment consists in the manner in which concepts are operationalised. To assess IQ, verbal or nonverbal tests are used, whose items address issues having different content, when to assess the facets of multiple intelligences specialised tests are used for each of them.

To outline the conceptual framework, we present the basic concepts with which we operate, as described in the literature, and especially the way they were adapted and accepted by the group of experts:

a) Verbal intelligence represents the ability to receive, process and work with words, to understand the relationships between concepts and to develop verbal reasoning, being necessary to:

- emit, receive and process some verbal messages;
- acquire some specialised theoretical and practical notions;
- collaborate with superiors and subordinates in diverse situations;
- understand instructions, conditions and safety measures during the execution of high risk activities.

b) Spatial intelligence represents the ability to determine the form, size, relationship and orientation of an object in relation to another object or a certain structure, being necessary to:

- develop some action strategies given concrete elements in the field;
- decipher the relationship between some graphical and practical elements, presented or displayed bi- or three-dimensionally;

- solve some practical situations in the field, which requires topographic orientation as well as the establishment of the size of objects or of the relationships between them etc.;
- place conventional signs on an action plan or a map.

c) *Numerical intelligence* represents the ability to work with numbers, to rapidly solve simple math problems, being necessary to:

- manage material and human resources;
- plan, manage, administrate and use some sums of money or budgetary funds;
- calculate the required materials and judiciously use resources.

d) *Organisational and bureaucratic intelligence* represents the ability to notice details, to accurately compare, evaluate and assess some products, programmes, plans, letters, words, and series of letters, to rapidly perceive and make decisions, being necessary to:

- develop, complete or record documents;
- organise, plan and perform military activities/actions;
- perform the act of command/execution;
- manage the military organisation;
- transmit messages and data via communication means;
- encrypt/decrypt encoded messages/information etc.;
- make rapid decisions in limit situations.

e) *Technical intelligence* represents the ability to understand the principles of mechanics, motion and force, the simple principles of physics, the relationships between objects and phenomena, being necessary to:

- know, maintain, and exploit the armament, technical means and equipment in the inventory;
- use the combat equipment judiciously, in relation to its characteristics and particularities;
- improve the equipment in the inventory.

f) *General learning intelligence* represents the ability to acquire knowledge and information to work with, being necessary to:

- develop skills and exploit the equipment, materials and human resources according to the standards required by position;
- adapt to new situations;
- understand, process and adapt information to concrete tasks;
- anticipate events and effects in different situations.

The third phase of research was aimed at developing items for each facet of intelligence (O3). In this phase, the group of psychologists, experts in selection, set the themes subsumed under the investigated aspect.

Subsequent to the study and the agreement expressed by experts, three thematic areas were established to collect and design the items within the tests to assess each facet, as follows:

- a) *the test to assess verbal intelligence* contains items covering verbal analogies, namely similar words (synonyms) and opposite words (antonyms), as well as logical-verbal reasoning;
- b) *the test to assess spatial intelligence* contains items covering the selection of some cut geometric bodies, some unfolded figures, and some objects in imaginary movement;
- c) *the test to assess numerical intelligence* contains items covering simple arithmetic calculations, series of numbers following a certain rule, and contextualised arithmetic problems;
- d) *the test to assess organisational and bureaucratic intelligence* contains items covering completing phrases, similarities between groups of letters, and the relationship between groups of letters following the *similarity* and *difference* criteria;
- e) *the test to assess technical intelligence* contains items covering some physical processes related to the movement of objects, levers, pulleys, and gears;
- f) *the test to assess the general learning intelligence* contains items that require identifying certain verbal similarities in a series of words, ordering notions in a logical succession, and continuing series of figures following a given rule.

Given the diversity of themes, a list of the formulated items was developed.

Subsequent to the *analysis of the concordance between experts* and the *validity of content* (expert method), the items that did not meet the quality criterion related to the initially established concept and thematic area were eliminated, resulting a number of 40 items for each facet and a total of 240 items for the entire battery.

The fourth phase of research was aimed at developing the *battery of psychological tests* compliant with the reliability and validity criteria (O4).

The resulted psychological tests were experimentally applied on a batch formed of 466 subjects, candidates for higher military education, post-secondary military education, and/or education/training programmes, aged between 18 and 40, with a mean age of 22,9.

Mention should be made that the batch meets the criterion of representativeness and is heterogeneous in terms of academic preparation, training, age and gender.

Each test was applied 2 times (10 minutes and 15 minutes), to establish the optimal time to complete it.

The data collected after testing were entered and processed in the *SPSS* (Statistical Package for Social Sciences) database. After verifying the correctness of data, we performed the analysis of items.

For accurate statistical results we coded responses to items as follows: the items correctly solved received code “1”, the items wrongly solved received code “0”, and the items not covered received code “2”.

We used this coding to verify, through statistical analysis, the normality of the distribution of responses for each item, and the internal consistency of items within each factor assessed. The main statistical indicators by which we checked these aspects were: mean, standard deviation and the coefficient of internal consistency Cronbach α .

Firstly, each item was analysed according to the mean and standard deviation, to check the compliance with the criteria of normal distribution. We defined the condition of isolation or elimination of items which mean was too large or too small compared to the theoretical mean and those with high dispersion, but for sure results they were not eliminated at this stage. The next operation was to calculate internal consistency coefficient Cronbach α . This statistical indicator shows, on the one hand, the impact each item has on the overall internal consistency of the analysed factor, the consistency of the set of items with the analysed dimension, and, on the other hand, the correlations between them. Following this procedure, indiscriminate items were eliminated, namely those having Cronbach α coefficient above 0,80 (very easy), below 0,20 (very difficult) and those that did not meet the criteria for a normal distribution, while checking whether, through elimination, the test homogeneity was not affected.

Finally, we took into account that the number of remaining items should be identical for each facet of intelligence. There resulted 120 items, 20 for each psychological test.

Analysing the values of Cronbach α coefficient, shown in *table 1*, for each facet, we can see that they have a high value, which guarantees that the developed tests are homogeneous (items are consistent in meaning) and one-dimensional (items are related to one dimension/factor).

By calculating Cronbach α coefficients, we checked the *reliability criterion* of the tests, namely “*the accuracy with which a test measures certain psychological characteristics*”⁸, using the method of “*inter-item consistency*”.

Moreover, the specialised literature mentions that “*a test with a high coefficient of internal consistency (Cronbach α) will have a high content validity if the particular*

⁸ C. Hăvârneanu, *Cunoașterea psihologică a persoanei*, Editura Polirom, Iași, 2000.

Test name	Crombach α Coefficient
Verbal intelligence test	Reliability Coefficients 20 items <i>Alpha</i> = .7771 Standardised item alpha = .7719
Spatial intelligence test	Reliability Coefficients 20 items <i>Alpha</i> = .6566 Standardised item alpha = .6502
Numerical intelligence test	Reliability Coefficients 20 items <i>Alpha</i> = .7570 Standardised item alpha = .7642
Technical intelligence test	Reliability Coefficients 20 items <i>Alpha</i> = .5884 Standardised item alpha = .6072
Organisational and bureaucratic intelligence test	Reliability Coefficients 20 items <i>Alpha</i> = .5909 Standardised item alpha = .5940
General learning intelligence	Reliability Coefficients 20 items <i>Alpha</i> = .7545 Standardised item alpha = .7592

Table 1

*factor is accurately described, and a very good content validity can provide a very good predictive or criterion validity*⁹.

With regard to *validity* or “*measurement quality*”¹⁰, literature in the field lists three basic methods as follows:

- *content validity*, which refers to the extent to which the formulated items are aimed at the content of the dimension/facet that is to be assessed;
- *construct validity* is the extent to which the measured factor can be assessed using other similar instruments (tests measuring the same facets of intelligence);
- *predictive/criterion validity* concerns the existence of some close and relevant relationships between the factor highlighted by a test and an external criterion.

Content validity was verified by two methods presented in the third and fourth phases of the research, namely:

- analysis of the concordance between experts regarding the content of items;
- elimination of indiscriminate items.

With regard to *construct validity*, it is applicable to the tests designed by the group of experts, being studied and analysed in terms of the results obtained by subjects in similar batteries in use in the selection and career orientation centres and applied to decision (AM1, AM2, AM3), using the correlation method by Pearson correlation coefficient.

⁹T. Constantin, *Evaluarea psihologică a personalului*, Editura Polirom, Iași, 2004.

¹⁰C. Hăvârneanu, *ibidem*.

Results are presented in *table 2*.

Test name	Correlation coefficient and significance threshold
Verbal intelligence test	AM1 : $r = .444^{**}$, $p = 0,001$ AM2 : $r = .444^{**}$, $p = 0,001$ AM3 : $r = .444^{**}$, $p = 0,001$
Spatial intelligence test	AM1 : $r = .539^{**}$, $p = 0,001$ AM2 : $r = .586^{**}$, $p = 0,001$ AM3 : $r = .471^{**}$, $p = 0,001$
Numerical intelligence test	AM1 : $r = .666^{**}$, $p = 0,001$ AM2 : $r = .672^{**}$, $p = 0,001$ AM3 : $r = .607^{**}$, $p = 0,001$
Organisational and bureaucratic intelligence test	AM1 : $r = .209^*$, $p = 0,005$ AM2 : $r = .360^{**}$, $p = 0,001$ AM3 : $r = .511^{**}$, $p = 0,001$
Technical intelligence test	AM1 : $r = .282^{**}$, $p = 0,001$ AM2 : $r = .380^{**}$, $p = 0,001$ AM3 : $r = .202^{**}$, $p = 0,001$
General learning intelligence	AM1 : $r = .539^{**}$, $p = 0,001$ AM2 : $r = .586^{**}$, $p = 0,001$ AM3 : $r = .471^{**}$, $p = 0,001$

Table 2

Analysing the values presented in *table 2*, we can conclude that, although there are significant correlations at a threshold of 0,001, the coefficient values are not high, and this aspect is due to the diversity of thematic areas regarding the content of the items in the experimental *battery*, compared to the batteries used for validation.

Moreover, we mention that, according to Colton¹¹, a correlation coefficient ranged between 0,25 and 0,5 represents an acceptable to good correlation. By analysing the content of the items in concurrent tests, we appreciate that the highest values for each test support the association of data and confirm the fact that similar constructs are assessed.

With regard to *predictive/criterion validity*, it is not applicable at present because of the lack of criterion, but it will be the goal of future research.

Finally, the fifth phase of research is aimed at establishing the final form of the *battery of tests* and at establishing the optimum psychological and aptitude profile (O5).

Based on the certainty that we obtained a *battery of psychological tests* that was discriminative, supported by observing statistical criteria, we established the final form.

¹¹ T. Colton, *Statistics in Medicine*, Little, Brown and Company, Boston, 1974.

Each test in the *battery of psychological assessment* should contain the description of the test, instructions, items, assessment and interpretation criteria, as well as the necessary elements to verify the results. To this end, we further present, to exemplify, some elements regarding the spatial intelligence (S.I.) test:

I.S. Test (spatial intelligence)

Test description:

It is a nonverbal test covering:

- the speed and accuracy to solve tasks having an image content;
- the ability to notice objects in motion/transformation (by rotating, cutting and assembling) and to work with algorithms;
- the development of two- and three-dimensional spatial representations;
- the power of observation, visual discrimination, imagination, logic and memory.

The test has 20 items.

The degree of difficulty is medium.

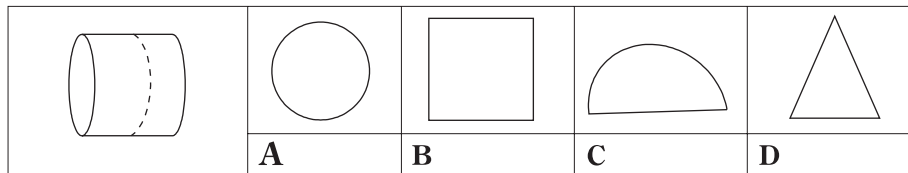
Instructions:

“There are 20 items in the test consisting of drawings containing series of figures, symbols and solids, for which tasks and answer variants are formulated. Answers will be written on the answer sheet. Work as quickly and accurately as possible. Time is limited. Start!”

Examples of items for each theme:

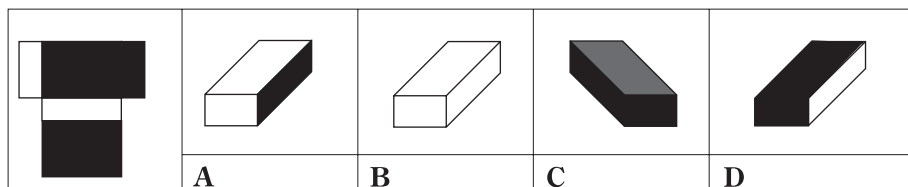
Example no. 1

On the left of the drawings below there is a solid cut by a dotted line. Following the section, it results one of the four figures in the series, denoted by letters from A to D. Which is the figure of the four marked with letters from A to D that corresponds to the section?



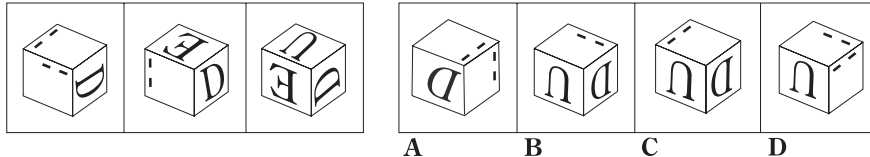
Example no. 2

What is the solid, out of the answer variants marked with the letters A, B, C and D, that results from the unfolded figure?



Example no. 3

The first three cubes rotate in a sense that should be discovered. Applying the discovered rule, you should identify the cube that follows in the series, out of the answer variants marked with the letters A, B, C and D.



Assessment and interpretation:

1 point is awarded for each correct answer. The *gross score (GS)*, representing the sum of the points awarded for each correct answer, is transformed into the *standard score (SS)* by reference to the general standard formula.

Interpretation and exploitation of results

In order to meet the last objective of the research study, the frequency of answers was analysed to establish the standard for the interpretation and exploitation of the results obtained by testing.

Moreover, to standardise tests, some elements of descriptive statistics were used: mean, median, mode, standard deviation, variance, minimum values, maximum values, vaulting and flattening indicators of the Gaussian curvature, as well as the frequency distribution.

The analysis of the statistical indicators and the frequency distribution shows that the results are generally distributed throughout the test range of values, following the criteria of normal distribution, with slight displacements, either to the left for N.I. test (average 6,63 and standard deviation 3,25), or to the right for V.I. test (average 12,27 and standard deviation 3,77).

For each test, the means and standard deviations are as follows:

- test V.I. – verbal intelligence – average 12,27 and standard deviation 3,77;
- test S.I. – spatial intelligence – average 9,80 and standard deviation 3,36;
- test N.I. – numerical intelligence – average 6,63 and standard deviation 3,25;
- test O. B. I. – organisational and bureaucratic intelligence – average 10,97 and standard deviation 2,87;
- test T.I. – technical intelligence – average 11,21 and standard deviation 3,15;
- test G.L.I. – general learning intelligence – average 10,81 and standard deviation 3,38.

According to the chosen military specialty (technical, logistical, humanistic etc.), the requirements of the job for which assessment is performed, and the total number of items, the test standards may be developed in 5, 7, 9, 10, 11 normalised classes,

by establishing minimal thresholds for admission or by designing optimal aptitude profiles.

The aptitude profile of a candidate is shaped by comparing the individual data and the optimal profile, agreed by the experts that conduct the psychological selection.

To exemplify, we present the concrete results obtained by a person assessed to be selected as follows: verbal intelligence, S.S.=9; spatial intelligence, S.S.=4; numerical intelligence, S.S.=4; organisational and bureaucratic intelligence, S.S.=8; technical intelligence, S.S.=4; general learning intelligence, S.S.=8.

The presented data show that the person has a set of abilities, intelligences or mental and cognitive abilities, called *facets of multiple intelligences, developed at the medium to upper level*.

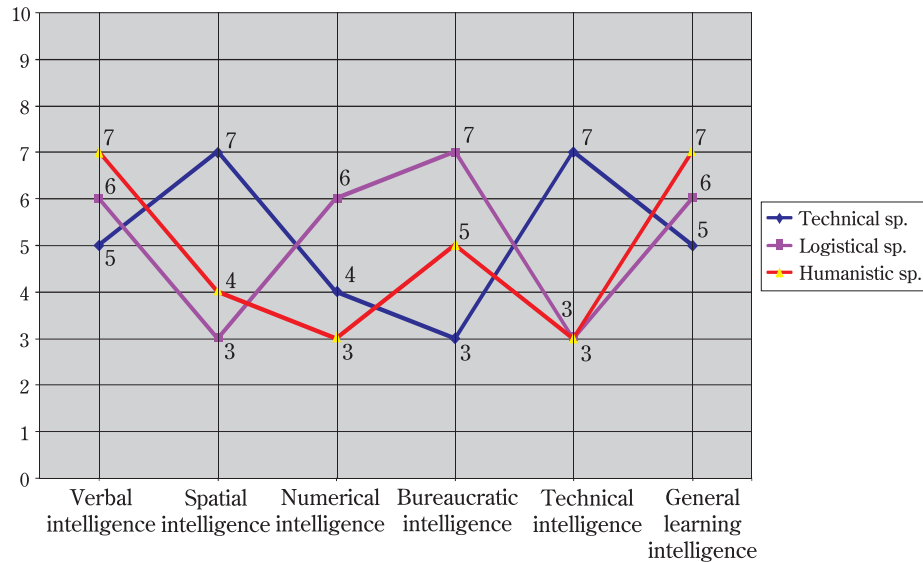
Out of them, the most remarkable are the following:

- the ability to operate and process the information having a verbal content, based on the vocabulary level and volume, flexibility, ability to find the verbal solution, the speed and accuracy to solve the assigned tasks orally/literally and/or with a verbal content;
- the ability to understand the relationships established between certain notions and to reconstruct mentally and practically the functions of some objects or facts, following patterns or codes contained in texts, verbal expressions or events/facts in progress;
- the ability to operate with figurative contents, to sense, to identify and determine some rules or their interference, based on their succession.

Secondly, at a lower level than the ones above, are the following:

- the ability to represent spatially, two- or three-dimensionally, the power of observation, and the visual discrimination, which entails the imagistic transformation from the three-dimensional plane into two-dimensional one;
- the ability to observe solids and their evolution in space, not only integrally, by rotating them, but also by performing sections, rotations or translations of the component parts, reflecting flexibility, the ability to find the spatial solution, the speed and accuracy in solving the assigned tasks having an image content related to solids or sections of solids;
- the ability to reason based on numerical relations and the evolution of some values obtained by multiplication or division, based on the information received in the form of series of numbers having different ratios or based on sentences that propose operations such the above-mentioned ones.

The results obtained by the subject are related to the optimal aptitude profile for technical, logistical and humanistic specialties presented below.



The person assessed initially chose to attend some training programmes in a specialty belonging to technical sciences. Following the results obtained and the profile shaped, by comparing them with the optimal aptitude profile, the person received vocational and educational counselling to change the option based on the new data available.

In conclusion, vocational counselling and guidance emphasises the ability of the assessed person to process and work with certain types of information or to solve a particular type of problems, based on identifiable operations or set of operations, highlighting the possibility that the person may obtain *very good professional results in the humanistic field*, contrary to the option for the technical field.

*

Psychology, as science, describes, especially through its applications, the person, both in the complex relationships with other human beings and especially from the individual perspective; people are all “*the same*”, but actually there are not two identical people in the world, and the differences are many, from anthropometric, physiognomic, vocal, fingerprint data to physical, occupational, intellectual, artistic and other aptitudes and abilities, due to the strictly personal experience related to growth/development and education/training. From this perspective, we are interested in measuring the traits and characteristics that make up the set of the ones that are necessary and sufficient in an activity or group of activities (i.e. profession or occupation) that are above par, and the ratio of the sum of the characteristics and the requirements of a profession or activity.

Joining a system of activities or group of professions that serve a particular technology/processing requires that individuals should possess and apply a set of aptitudes and interests in synergy with the goals of the organisation, and that the professionals who perform the selection/psychological assessment to establish and maintain the human resource at the projected standards should apply a common measurement for all people and their aptitudes, but describe performance separately and in a specialised manner so that the selection results/conclusions can lead to distribution/education/training.

It is known that the activity in organisations requires the presence of specific individual characteristics to achieve higher returns, hence the necessity to develop a battery of tests to capture, ever since the selection, “*the aptitude potential specific to a profession*”, namely the aptitudes considered important for the job performance and training.

Selection is one of the first steps in a comprehensive approach that has as main objective the enhancement of the candidates’ effectiveness in performing the institutional tasks at high standards. To obtain maximum efficiency and superior results in the activities performed in organisations, the selection and human resource decision makers should take account of the specific skills potential, knowing that its development throughout the career leads to the optimisation of the particular activity.

We have developed a unique *battery of tests* for assessing human resources at all levels, for general, medium-specialised and specialised execution activities, the latter including the requirements for managers up to the top level of the organisation pyramid. Its components (subtests) consider six specific facets, namely verbal intelligence, numeric intelligence, spatial intelligence, organisational and bureaucratic intelligence, technical intelligence and general learning intelligence.

Applying this objective and standardised tool, such as the *unique battery of tests*, provides the opportunity to scientifically, objectively and really know the potential of the human resources that candidate for joining an organisation, as well as throughout the career, because of the variants that are specific to the stages and assessed professional categories.

The studies meant to validate the *battery* confirmed its reliability, homogeneity and prognostic value, and established the standard application times.

The curvatures describing the performance of the subjects in the group/population under research, for all subtests, highly correlated with the criteria established by experts and validated the *battery* as a predictor of the assessed human resource job performance.

English version by
 *Diana Cristiana LUPU*

SPACE AS MILITARY ENVIRONMENT

– Between Law and Power –

Lieutenant Colonel Dorian LUPARU

The author writes that the dominant challenge regarding the future of space consists in the existence of two concurrent visions, focused on the way in which space activities should be organised, managed and controlled. After detailing these two visions, he approaches the current legal framework regarding space, which is more and more fragmented and inadequate to meet the challenges posed by the increasing use of space, pointing out the need for a new and comprehensive legal framework.

Then, he poses some major questions regarding space weapons, in terms of priority target for investment and the best approach to counter actual or potential enemies, to which answers can be given after thorough analyses, with global and strategic vision. In his opinion, we will witness certain decisions that will definitely affect our planetary future: law or power in space.

Keywords: *terrorism; space treaties; satellite communications; NASA; vulnerability; threat*

Motto:

“Control of space means control of the world”.

American Vice President Lyndon Johnson, 1961

M

ore than 60 years after the explosion of the first nuclear weapon, the “*nuclear club*” has grown from one nation to nine, but no nuclear weapons or, better said, no weapons of any kind have been launched into the orbit all this time. Space remains a weapons-free zone, although not a military activities-free zone.

While the world is preoccupied with the “*war on terror*”, the US has advanced the capabilities development plans regarding “*space control*” and “*global engagement*” – euphemisms for weapons in space. Since 9/11, this issue and the one related to the ballistic missile defence have made the headlines less and less, even if, in my opinion, they deserve much more control and public attention.

Currently, the military use of space takes place with the purpose of communication, through surveillance satellites global positioning

Lieutenant Colonel Dorian Luparu – “*Division General Constantin I. Brătianu*” Topogeodesic Provision and Training Unit, Buzău.

systems, in the service of everybody. If one nation were to “*break the ice*” by launching weapons into space, it would provoke a competition for space superiority almost certainly dominated by the United States; even the development of ground based *Anti-SATellite Weapons – ASAT* would represent a serious departure from daily practice. In this respect, a concerted international effort is required in order to develop a more comprehensive legal regime for space, which will limit its uncontrolled weaponisation; otherwise, the military competition that might erupt in space will have serious consequences, which are destabilising for global security. Besides adding to the existing threats of armed conflict, it will jeopardise the broad range of scientific and commercial uses of space and will put itself at risk by the extensive military use of space.

New international agreements, under the aegis of international legislation, are also required, not only to limit what can be placed in the orbit and what can be the purpose of objects in space but especially to distribute most equitably the benefits of space activity. Now, space serves enormously the commercial, scientific and military communities all over the world and, without these new agreements, its use may be mostly shaped by the short-term interests of power to the detriment of the long-term interests of the humankind.

The Current Challenge: Law versus Power in Space

The dominant challenge to the future of space lies in the existence of two competing visions regarding the way in which activities in space should be organised, managed, and controlled.

The *first vision* emphasises the central role of law in preserving space for “*peaceful purposes*”, promoting international cooperation in using and exploiting space to the benefit of all. This vision underlines the benefits of an international legal regime, as being the best way to balance the various interests in space, to manage the possible interference of activities and to make sure that no single power can gain a dominant position, thus jeopardizing other people’s access to space. Power is this way constrained by law, and national interests are pursued by assuming mutual interests. This vision establishes the logic of the creation of a legal regime for space (even if it is weak and incomplete), reflected in a set of outer space, weapons control and commercial treaties and agreements that began in the 1960s¹.

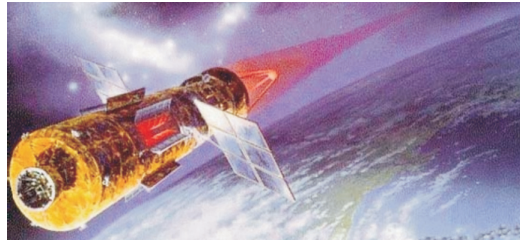
¹ The Nuclear Test Ban Treaty, in 1963, which bans nuclear weapons tests or any other nuclear explosion, in space; the Outer Space Treaty, in 1967, which bans weapons of mass destruction in space, on the Moon or on other celestial bodies; the Anti-Ballistic Missile Treaty (ABM), in 1972, which bans the development, testing or deployment of space components of anti-ballistic missiles systems.

The *second vision* is the one of the dominant nation, as formulated in a project of *US Space Command (US-SPACECOM)*. Considering that the American government has an increasing interest in the space, for both the commercial and the military domain, *SPACECOM* has maintained that US satellites are vulnerable to attacks, therefore, the United States needs to dominate space militarily. In fact, the Air Force doctrine stipulates that *“the environment of space is the fourth environment of warfare – along with land, sea and air..., which must be protected and controlled”*².

SPACECOM's Vision for 2020 (laid down in 1997)³ argues that the protection of space requires superior US space combat capability and proclaims that the US military are *“stewards for military space”*. General Joseph W. Ashy, a former commander of *SPACECOM*, argued that the United States *“will engage terrestrial targets someday – ships, airplanes, land targets – from space. We will engage targets in space, from space.... The missions are already assigned, and we’ve written the concepts of operations”*⁴. Moreover, *SPACECOM* claimed that the United States must establish a military presence in space in order to anticipate the possible efforts by other nations to do so.

Although this is only a vision of *SPACECOM*, in recent years, it has been brought again to attention by civilian defence officials, who have begun to implement changes in the Pentagon doctrine and to align budgets with the second vision of space, which is sometimes called the *“global engagement strategy”*.

Approximately ten years ago, the Rumsfeld Commission report on the management of US space assets, produced by a study commission chaired by Donald Rumsfeld, before he became Secretary of Defense, signalled its total support for the *need to project force in space*, in order to counter potential threats to US military security there. The Rumsfeld Space Commission, one of the most influential in the US Senate, concluded that space interests were a top national security priority and that the USA must further ensure superiority in space capabilities in order *“both to deter and to defend against hostile acts, in and from space”*, including *“uses of space hostile to US interests”*⁵. The Commission supported the need for transforming



Space laser provides a powerful impulse of energy enough to destroy missiles in flight

² US Department of the Air Force, *Space Operations, Air Force Doctrine Document 2-2*, Washington, DC.

³ US Space Command, *Vision for 2020*, 1997, at <http://www.fas.org/spp/military/docops/usspac/visbook.pdf>

⁴ W.B. Scott, *USSC Prepares for Future Combat Missions in Space*, in *Aviation Week and Space Technology*, 5 August 1996, p. 51.

⁵ Lieutenant Colonel Donald P. Christy, *United States Policy on Weapons in Space*, US Army War College, Carlisle Barracks, 15 March 2006.

American military capabilities and upgrading them to provide efficiency, modernity and productivity in order to maximise US space control capabilities and to deny the enemies such capabilities. In this respect, seven missions were specifically identified: *assured access to space and on-orbit operation; space situational awareness; earth surveillance from space; global command, control and communications in space; defence in space; homeland defence; power projection in, from and through space.*

In late September 2001, the *US Quadrennial Defense Review*⁶, an ample assessment of US defence policy, demanded the strengthening of military space surveillance, communications and other applications of spacecraft, all in keeping with the current regime. But it went further, highlighting the need to deny the use of space to the enemies and arguing that US vulnerabilities in space must be balanced with the aggressive development of added space capabilities. Most tellingly, *The Department of Defense's Nuclear Posture Review*⁷, fragments of which were *leaked* in March 2002, advocated the use of satellites in order to enhance conventional and nuclear strike capabilities.

In October 2002, *SPACECOM* merged with the *US Strategic Command*, which controls US nuclear forces, to create a single entity responsible for early warning, missile defence and long-range strikes. The Pentagon requested 1,6 billion dollars over the investment plan 2003-2007 in order to develop lasers in space and the so-called *kinetic kill vehicles* to intercept and destroy ballistic missiles (as well as satellites). In November 2003, the Air Force released a report, which, for the first time, offered detailed descriptions of planned anti-satellite weapons. This suggests a certain quiet movement towards the deployment of weapons in space⁸.

Providing further signs of high-level support for the global engagement strategy, the Bush administration's decision to withdraw from the *Anti-Ballistic Missile (ABM) Treaty*, in June 2002, which was thirty years old, appeared to be determined less by technical needs of anti-missile defence testing (testing could be done within the terms of the treaty, and the deployment of a feasible system was not imminent) than by a desire to eliminate inconvenient legal obstacles to projected US power in space.

In October 2006, President Bush released a new national space policy, which supported the US unilateral freedom of action in space. The US must be able

⁶ Department of Defense, *Quadrennial Defense Review Report*, September 2001, at <http://www.defenselink.mil/pubs/qdr2001.pdf>

⁷ Department of Defense, *Nuclear Posture Review*, 2001, at <http://www.globalsecurity.org/wmd/library/policy/dod/npr.htm>

⁸ US Air Force, *The US Air Force Transformation Flight Plan*, 2003, at <http://www.af.mil/library/posture/AF-TRANS-FLIGHT-PLAN-2003.pdf>

to “deny, if necessary, adversaries the use of space capabilities hostile to US national interests”. Although not explicit in the document, this is an opening for the development and use of weapons in space. The new policy also warns that “the United States will oppose the development of new legal regimes or other restrictions that seek to limit or prohibit US access to or use of space”⁹.

Even President Obama admitted, during his presidential campaign, that a global treaty for banning weapons in space could be a discouraging challenge. A simple and more rapid solution, as he suggested at that time, would be a “code of conduct for responsible space-faring nations”.

Although the Air Force, the agency that manages US activities in space and its supporters strongly assert their points of view, this assertion may be only premature when they consider that they advocate US policy. Funding for space weapons has not yet followed rhetoric. Even in the Pentagon, the opponents of weapons in space outnumber the advocates. Many officials in the military – as well as in NASA and the Congress – are aware that the interests of the United States in space are much broader and the weaponisation of space could add risk to the other uses of space. The support of the Congress for space weapons programmes is difficult to assess, but does not appear to be deep or widespread. The programme tends to be popular among conservatives in the Congress, but not among democrats or moderates. On the other hand, the support for an anti-missile system is broader.

The risks involved by a competition for national dominance in space would be substantial for many nations, but especially for the United States. The Americans are by far the nation most reliant on space, for its military and economic interests. The USA has in the orbit an estimated 850 satellites, both military and commercial ones, a number that is expected to increase considerably during the next 10 years. Although, in the short term, the technological and financial allocations in space will grow, ultimately, the United States will see that advantage diminish. Thus, in the case in which the USA aggressively supplies weapons in space, it will possibly cause other nations to begin countermeasures, with destabilising consequences for world and national security. By encouraging nations, which are not interested momentarily in sending weapons in space, to develop programmes in this respect, the USA could lose the advantages it seeks to protect.

According to most of the rest of the world, especially China and Russia, this vision of national dominance is incompatible with the legal system established in the present for space. For over 40 years, the international community has repeatedly stated that space should be preserved for peaceful purposes, made available

⁹ *US National Space Policy*, 31 August 2006, at <http://www.fas.org/irp/offdocs/nspd/space.html>

to everybody and be weapons-free. A competition for superiority in space could put an end to the right for using it, one that now benefits all nations, in turn, it could create a *de facto* regime of control on access and use by a dominant nation in order to deploy space weapons or anti-satellite ground weapons. Considering the huge value of outer space and its resources, other nations could develop their own anti-satellite weapons, designed to break this monopoly, and the countries that do not possess the capabilities for building such weapons might buy them.

A more elaborate legal regime should focus on preventing destabilising conflicts aimed at using space. Currently, the USA can stand against any other nation, and the support of some allies, even close ones, is rather questionable. However, forcing space domination might be counterproductive for national interests. The traditional military support activities (space-tracking, early warning, communications, reconnaissance, weather, and navigation) will be in danger. The commercial and scientific activities in space would be exposed to serious risk as well; thus, in a conflict, terrestrial components of space activity could become targets, while attacks against satellites could cause a disorder in space because of the debris that might collide with them, disrupting commercial and scientific activity and communications on the ground.



An arms race with anti-satellite weapons is one of the dangers: a convincing example in this respect is China's first successful test of an anti-satellite missile on 11 January 2007¹⁰. The test consisted in destroying an inactive Chinese weather satellite by a kinetic kill vehicle, launched by a medium-range ballistic missile. The *ASAT* weapon intercepted the target at an altitude

of approximately 530 miles, which was consistent with the operational altitudes of American and Japanese imagery intelligence satellites. Possibly as a response, the Americans carried out a similar action a year later, when they destroyed one of their satellites, claiming that its tank, containing toxic fuel, could be dangerous if it were to fall on the ground. Mention should be made that the first action of this kind took place in 1985 on the part of the USA.

¹⁰ Craig Covault, *Chinese Test Anti-Satellite Weapon*, in *Aviation Week & Space Technology*, 2007.

Of even greater concern for nations such as Russia and China is the US use of space systems to improve its nuclear and conventional strategic strike capabilities. From the perspective of these nations, a US decision to expand strategic capabilities in space would represent the collapse of the *Cold War* understandings regarding strategic stability based on mutual vulnerability. A military competition in space could invigorate the arms race by high technology and could renew emphasis on nuclear warfare doctrines.

Since 1999, China and Russia have used diplomacy means to try to obtain, at the Conference on Disarmament, the beginning of negotiations regarding a new treaty to ban weapons in space. Seeing in retrospect the constant refusals on the part of the USA, one must not neglect the fact that both seem to have and develop technologies in order to counter, neutralise, avoid or even attack any potential threat on the part of the USA, in or from space.

Eventually, a military competition in space would largely extinguish the role of law in space in favour of a regime of power. Despite the appeal of the advocates of “*space control*”, the broad interests of the United States in space lead to the promotion of a legal regime. The United States has a long history of advocating the rule of law in affairs both nationally and globally, as well as in promoting the development of rules that would secure US interests in an interdependent world. Choices will have to be made, and when that time comes, it is likely that most users of space – including the satellite communications industry, with the support implications in military operations and the scientific community, including NASA – would prefer a stable protection provided by the rule of law to the uncertainty and potentially disrupting protection of complex, untested weapon systems.

The Current Legal Regime

The need for a new and comprehensive space legal regime lies in the fact that the current one is increasingly fragmented and inadequate to meet the challenges regarding the increasing use of space. It consists of some general principles expressed in five space treaties adopted since 1967 and an arms control treaty, in keeping with general international laws and the practices of the space nations. The legal regime also includes various agreements covering the commercial uses of space, such as rights to use geostationary orbits, and agreements establishing inter-governmental organisations in areas such as telecommunications, civil aviation, and weather.

The general principles include the idea that space should be reserved for “*peaceful purposes*” and that no nation can claim dominion over any part of it.

However, because only a small number of countries are now capable of carrying out activities in space¹¹, these principles have not really been tested and remained aspirations. The definition of “*peaceful*” is contested and unclear, the concept of environmental protection for outer space is insufficient and there is no agreed-upon, operational definition of the concept of “*province of all mankind*”, a term used in the *Outer Space Treaty*.

With regard to “*peaceful uses*”, the current legal regime imposes some limits on military activity in the vacuum, in the near-Earth space, and bans all military activities on the Moon and other celestial bodies. Although nations, through the UN, have declared that outer space should be reserved for “*peaceful purposes*”, the space powers have interpreted this by *permitting* “*passive*” military support activities, such as surveillance, communications and detection of missile launches or nuclear explosions on Earth. The language of the major treaties has been carefully chosen so as not to ban the passage of nuclear ballistic missiles through space. In truth, despite a huge and increasing use of space, for commercial and scientific purposes, the military use is still dominant. A very beneficial effect is probably the use of satellites to monitor US-Russian arms control agreements.

Therefore, despite some important interdictions on military activity in space, the current legal regime comprises significant gaps. It bans the stationing of weapons of mass destruction, including nuclear weapons, in space, but allows the deployment of anti-satellite weapons on the ground and the placement of conventional weapons in orbit. Nothing prohibits the launching of nuclear weapons from Earth in space for the purpose of destroying enemy missiles, therefore, as permitted by the 1972 ABM Treaty, the US and the USSR deployed missile defence interceptors (in North Dakota and around Moscow, respectively).

An Asymmetrical Analogy between the World Ocean and the “High Frontier” of Space

Space arming has been, for some, both a natural progression, in order to provide multiple layers for ballistic defence missile (land, sea, air and space, described as “*the fourth environment of war*”), and an objective in itself. American supporters of space arming, responsible in 1996 for approximately 64% of global spending

¹¹ Countries with launch capabilities, therefore, with the technical infrastructure to put weapons in space: USA, Russia, Ukraine, China, India, Israel and France/ESA (members of the European Space Agency, which use the *launch* site in French Guyana). Others have ballistic missiles capabilities and an increasing number have significant military assets in space to support their military forces.

on commercial use of space and over 90% of global spending on military space assets, have given three reasons for their vision:

- *control* – control of space gives huge and unmatched military and commercial advantages;
- *vulnerability* – resorting to space assets has particular vulnerabilities;
- *unavoidability* – in terms of evolution, weapons in space follow weapons on land, sea and air (the historical analogy of projecting force at sea and in the air – “*trade follows the flag*”, regarding the military development in terms of protecting commercial expansion). The main concern of the USA is the dependence in terms of its combat military space assets, in relation to land conventional warfare; there is fear and vulnerability that a potential enemy may use anti-satellite weapons (ASAT) to neutralise the USA’s dominant military position or even to create superiority in relation to US forces. This is essentially a “*Space Pearl Harbor*” scenario used by the Rumsfeld Commission to extremely illustrate the space arming option¹².

Taking advantage that there are gaps in the legal regime to prevent the weaponisation of space, space weapons supporters invoke an analogy between “*World Ocean*” and the “*High Frontier*” in space to justify their position. Space, they say, is like the World Ocean, beyond the control of any nation. Under the traditional principle of “*freedom of the seas*”, nations cannot claim sovereignty over any part of the World Ocean, but are free to use it, including for military purposes. Similarly, the advocates of weapons in space share the opinion that the USA should be free to place weapons (of any kind) in space, just as it can keep a fleet of submarines and patrol warships across oceans. “*Pax Britannica*” is the favourite image: just as, in the nineteenth century, Britain ruled the waters under the principle of freedom of the seas, in the same way, now, a power can regulate space. Just as the merchant navy needed escort ships, the argument continues, commercial satellites will need protection and military escort in the future.

The analogy has a coherent appeal, but it can be considered misleading. In fact, freedom of the seas is no longer a useful guiding principle for the World Ocean, much less for space. The concept may have been appropriate for the 19th century world, in which it arose, but is inadequate for managing the complex challenges to the oceans, in an extremely interdependent world. Essentially, the principle of “*laissez-faire*” has opened the past to unilateral interpretations, leaving the World Ocean vulnerable to overuse, pollution, military activities and other uses etc. Space, like the World Ocean, is not limitless, it does not have an infinite capacity to absorb

¹² W.B. Scott, *lucr. cit.*

activities. The space segment is reduced, available for geostationary or orbit satellites, and the increasing quantity of debris in near-Earth space places serious physical limits on space activities. Moreover, military activity in space, just as the one in the World Ocean, could anticipate other uses.

There are other arguments invalidating the analogy between the World Ocean and the “*High Frontier*” of space. The military threat posed by space weapons could become even greater than the one posed by weapons on or under the World Ocean. The transit of weapons in space is not as “*innocent*” as the transit of the oceans, considering the speed and vulnerability of space weapons, and satellites are not like ships, needing escorts. The role of a power in space would be far more dominating than the role of Great Britain during the 19th century. It is difficult to avoid the conclusion that, in reality, one can employ a version of *mare clausum* (closed seas), in which most of the control in space would belong to a group of powers or even to one single power. The reference to the freedom of the seas analogy is, in the end, relative: the relation to the British example of the 19th century tends to underline the aspect of dominance rather than the freedom of the seas principle. The doctrines centred on control and domination are not theories of free trade and commerce.

What Are the Solutions? The “Space Sanctuary” Regime?

An extended, elaborated regime for space will require a shift from a framework based largely on a freedom of the seas analogy to the notion that security is achieved based on the principles of *comprehensive security, equal protection in space, and equity in the use of space resources*. A broader definition of space security would go beyond a purely military approach, to include aspects regarding resources and environment, as well as economic and development concerns. Such an approach is crucial for space, which affects many (in some ways, all) nations and the planet as a whole. Military approaches, environmental aspects and economic issues are interconnected in space. Just to give an example: testing ASAT weapons in space could produce thousands of pieces of debris, which would cause risks to commercial, scientific, or military satellites from low-Earth orbits.

Policies for space will also need to reflect the *principles of reassurance to the detriment of threat and deterrence stratagems*. They will need to address the issue of uneven distribution of security and protection among nations. For instance, the USA possesses great capabilities to wage war, greater in terms of proportion to what other nations possess. This huge asymmetry creates incentives for opponents to wage a different kind of warfare. Now, when proliferation of nuclear weapons,

terrorism and unconventional warfare pose major security threats rather than an attack from another state, the traditional concepts of deterrence and confrontation are increasingly dysfunctional and even counterproductive. The long-term stability of the space regime depends on its organisation as a regime of collective protection of nations and space assets rather than as a regime of threat and deterrence organised at national level.

The principles of equity, responsibility and fairness in the use of resources will also need to be central elements of an elaborated space regime. Space is indeed the “*province of all mankind*” and the international community should have a say in the way it is used, as well as in the benefits that derive from its use. At a minimum, these principles imply that there must be limits to freedom of use, especially in case of war. The rules of space will need to reflect world interests rather than national public interests of a few space-faring governments and corporations.

These principles will need to harmonise the content through specific operational rules. The definition of “*peaceful purpose*” needs to be clear, and, in our opinion, one must set certain limits on the freedom of exploration beyond the Earth. Though total demilitarisation of space will remain the aspiration of many nations and groups, it is unlikely that this will happen. Instead, it is very likely, almost inevitable, that space will continue to be used for passive military purposes. That is why, a clear definition of “*passive*” will be required.

A regime that recognises some military use of space, but not its weaponisation, is often called a “*space sanctuary*” regime. It would prohibit the testing and deployment of weapons in space, as in the case of ASAT weapons on Earth and would formalise what has been, for nearly fifty years, an informal understanding among nations. Despite the lack of progress regarding weapons control in space, the most remarkable feature of the current regime for space has been the tradition of restraint in weaponising space. The international community has repeatedly reaffirmed its support for non-weaponisation as a norm, in numerous UN resolutions and diplomatic statements. Time may be a good ally for formalising the notion of “*space sanctuary*”.

A prohibition on weapons in space would allow ballistic missile trajectories through space, but not weapons placed in orbit. This means that, according to the “*space sanctuary*” rules suggested above, anti-missile defence would have to be ground-based, and not space-based.

A second essential rule of the regime would be a ban on the interference with space assets. Satellites that perform “*peaceful*” missions and security-related functions, including agreed-upon military support activities, together with their ground-based support installations, would be declared beyond the limits of an attack. The interference

with the space assets would be viewed as an aggression, and the violation would trigger strong sanctions or penalties. Most nations would have a strong interest in preserving the immunity of own space assets from a possible aggression, that is why, pursuing own interests and the threat of retaliation would contribute to sustain the rule.

However, it is easy to abuse the non-interference rule (such as freedom of the seas). Freedom to do anything can mean, on the one hand, freedom to disregard the interests of other parties. Therefore, it will be important to mention what activities are beneficial for non-interference. In space, this means clear rules about the limits of military support activities, which are currently unrestricted. The central issue is the role of satellites in supporting ground weapons; some of their uses, such as the identification and location of targets for long-range precision attack, missile guidance, and conduct of offensive ground operations, can be considered very aggressive. Thus, without clear constraints, space could be used to increase the lethality of ground-based weapons, including nuclear weapons.

The need for clarification has become stringent because of conflicting interpretations of the current legal regime, especially between the United States and China, in terms of defining the types of military support activities that are “*peaceful*”. Even without weapons in space, we strongly need rules on the limits of satellite activities, based on their purposes and observations in support of military activities.

These rules will need to be designed to reassure all parties that space surveillance practices, used to verify compliance with treaties, are not part of a clandestine ABM plan or for espionage! The nations with space programmes will need reassurance that the adversaries are not developing space capabilities in order to launch the first strike and that unilateral deployments are not a cover for aggression. Moreover, it would be necessary that the new rules prevent the secret weaponisation of space, as well as the domination of space by military activities to the detriment of other uses. These may bring about some form of cooperation for monitoring and early warning of missile launches.

Some nations were against any negotiations on banning space weapons, in the Geneva Conference on Disarmament, as well as during the UN’s multilateral arms-control forum, maintaining that existing arms control agreements were adequate. Thus, the creation of an improved regime for space will likely be required by interested nations, non-governmental organisations, commercial enterprises and other structures interested in the space. They must lead the synergy, constraining together the political activity and the activities in space.

Are Space Weapons Inevitable?

The decision to place weapons in space is a choice, not certitude. Those who argue it through human nature, historical analogies, economic vulnerabilities or military necessities lead to the theory of unavoidability of space weapons. Each of these arguments deserves attention but neither of them has a sufficient importance to advocate the unavoidability of weapons in space.

The argument of *human nature* affirms that humans have an aggressive side, they are warriors and the nations they lead will serve their national interest, which naturally includes the purchase of weapons, space one included. The implication is that people cannot control their tendency of developing or implementing any weapon, which could benefit them military, really or distinctively in terms of an enemy. However, mention should be made that, for the past fifty years, the outer space has been weapons-free. People and nations have resisted to the temptation so far.

Regarding *historical analogies*: people wandered on the World Ocean, in the air and under the oceans and, in each case, they weaponised and armed these environments. Then, why should we expect a different attitude for space? General Howell M. Ester III, former chief of *SPACECOM*, contributes with the following reasoning: *“If we examine the evolutionary development of the aircraft, we see uncanny parallels to the current evolution of spacecraft. The potential of aircraft was not recognised immediately. Their initial use was confined to observation. Until one day, the full advantage of applying force from the air was realised and the rest is history”*¹³.

Another argument for placing weapons in space is the threat to *economic* dependence upon space of a nation, which is increasing, in other words, economic vulnerabilities. Following this logic, space assets become a target for a potential enemy, therefore they require capabilities for their defence with space weapons. In this case, there are two serious questions that can be considered:

- 1. How high is the price of defending those assets with space weapons as compared to the price of the assets itself?*
- 2. Most space military systems are much more expensive than the civilian satellites they would protect, but which is the probability that space assets are targeted by an enemy?*

Most civilian systems or systems with significant economic value operate in very high orbits (between 11 000 and 24 000 km). *Why would they be easier targets than military reconnaissance satellites that operate in low-Earth orbits?*

But, why would an enemy threaten such kind of systems?

¹³ *Ibid.*

Probably, the purpose would be to cause major economic and limitation damages. Most space economic assets have ground alternatives, such as optical fibre communications or ground navigation support, that is why it seems that space assets are a less tangible target, considering the technical capabilities necessary to damage them decisively, and especially due to the fact that precision would be difficult to achieve. And in a world economy that is extremely globalised, the deterioration of space infrastructure would most likely affect the economy of only one nation, let us say the United States. Going through this logic, there are numerous Earth objectives that may involve, for a potential aggressor, an effort significantly reduced.

Regarding Space-to-Earth Weapons, the United States already has the capability to project considerable force around the Earth. Space-to-Earth Weapons could provide an advantage in the quickly striking capability, over existing capabilities, but is this a completely convenient solution? Prompt and precise strikes in the war in Iraq, “*targets of opportunity*” could not get Saddam Hussein out; the attacks against terrorist leaders in Pakistan were not successful; even the strikes from space will require the support of accurate information on the ground. In other words, a sniper on the ground, with a 500 dollars rifle, could perform the same task as a satellite of 500 million dollars, in space, which would further require human land links that would provide information support.

That is why, serious questions are posed in order to establish if the threats to satellites are founded and, even if the threats are real, the weapons based in space, which are expensive and complicated, would truly be the most efficient solution. In many cases, it is likely that a potential enemy uses more efficiently and easily the attacks on Earth targets.

The argument as *military necessity* underlines that the military advantages of space weapons will soon be so big, that acquiring them will be in the interest of national security¹⁴. Space weapons will “*defend friendly satellites, attack enemy space weapons and other satellites that perform important military functions, shoot down long-range ballistic missiles and conduct attacks against enemy air and surface forces*”¹⁵.

The basis of this argument is that no matter what a nation chooses to do, other countries will certainly develop weapons in space in time. The US depends a lot upon the force of the aspects of enhancement of its military satellite systems,

¹⁴ Karl P. Mueller, *Is the Weaponization of Space Inevitable?*, 27 March 2002, at <http://www.isanet.org/noarchive/mueller.html>

¹⁵ *Ibid.*


including communication, navigation, warning and reconnaissance ones: “We cannot afford that another space power paralyses the advantages provided by these systems. Beyond economic arguments, our military space systems are indispensable”¹⁶. The counterargument of this theory emphasises that the lack of interest for the development and deployment of space weapons finds its response in vulnerability.

*

The current challenge to the international community in space today is the collapse of a nearly 50-year tradition of restraint from military activities in space. The US plans for the “*Global Engagement*” may represent the concept of restraint, in favour of a unilateral regime of assertion of power, which can largely affect the interests of others. The lack of a legal order in space may jeopardise the interests of all nations in space, irrespective of their place and role in the hierarchy of capabilities in orbit.

Unilateralism will not be quietly accepted. One way or another, a new regime for space will emerge, because the existing regime cannot survive. Either it will be transformed, by agreement, into a more elaborated regime, which will balance various interests in space by establishing new and modern guiding principles and new, clear norms, or it will be implicitly transformed into a regime of power and an arena of military competitions.

Today, there are more space-faring countries than there were in the 1960s and 1970s that are in a position to influence the issues and to counter US freedom of action through various kinds of interference, such as jamming satellite signals. It would be ideal to accept that security in space will be more effectively achieved through a rule-based system than through the deployment of destabilising weapons systems. Most countries in the world do not rush to weaponise space and appear ready to find comprehensive solutions and new rules to govern space activity. In the long run, the best way to protect commercial, scientific, and security interests in space will be through the stability of the rule of law, obviously more advantageously than the unilateral assertion of military power.

English version by
 **Iulia NĂSTASIE**

¹⁶ *Ibid.*

THE PEOPLE'S REPUBLIC OF CHINA CYBER CAPABILITIES

Major Marian LAZĂR

The author discusses the importance the Chinese leadership has attached to information technology lately.

In this respect, the Chinese modernisation effort is emphasised. This sustained effort has led to a radical transformation of Chinese military concepts and architecture, in terms of C4ISR infrastructure, information warfare capabilities, IT research for military purposes. Moreover, the structures in charge of cyber domain are mentioned, and their main activities are listed, as they result from the analysis of numerous public sources.

In conclusion, it is shown that China intends to stand out and remain among top states in terms of possession and use of cutting-edge cyber capabilities.

Keywords: *cyber capabilities; information warfare; cutting-edge technology; C4ISR*

T

he Chinese government has paid special attention to the IT domain over the past 20 years. To denote

the transformation process that is underway in China, Western scholars have used the term *informationisation*¹. The Chinese modernisation effort aims to develop a network-based architecture, capable of coordinating military operations on land, in air, at sea or in space.

This sustained modernisation effort has led to a radical transformation of Chinese military concepts and architecture, creating a modern and globally competitive infrastructure for command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR). The emphasis on the development of a modern C4ISR has triggered, in turn, a modernisation process related to specific information warfare capabilities able to protect own computer networks, either military or civilian, and to ensure control on adversary information systems during a possible conflict.

Major Marian Lazăr – the General Staff, the Ministry of National Defence.

¹The concept of *informationisation* refers to the informatisation of all areas of social activity: military, industry, education, culture and even agriculture.

IT research for military purposes is very important to Chinese political and military leaders. It is known that more than 50 civilian universities currently receive research grants to the immediate or potential benefit of the armed forces. The Chinese People's Liberation Army has various contracts with major civilian companies in the field of communications, thus having access to cutting-edge technology. Instead of blocking the activity of companies conducting research solely in the interests of the army, military leaders prefer these companies to have access to foreign products and to have partnerships with other companies in the industry outside China, thereby ensuring access to their technology. In some situations, China's interest in technology other than domestic resulted in penalising foreign companies, as it was the case of Sun Microsystems in the United States, which, in 2003, was fined about 300 000 dollars for the illegal export of computer components that were used for military purposes by China².

The Chinese People's Liberation Army leaders have understood the utility of cyberspace control and possession of tools able to affect adversary information systems, even by preventive strikes.

The Chinese army has not disclosed the existence of a strategy for operations regarding computer networks and currently it seems to be in the process of integrating all the components that can be associated with information warfare (electronic warfare, psychological operations, disinformation and so on) into a broader concept, that of "*information confrontation*".

Although China does not have an independent strategy regarding information warfare, it has several *military strategic guidelines* that articulate key orientations regarding defence policy in the field of information warfare and establish directions for modernisation. These guidelines have been updated only 5 times since 1949. The last modification, in 2002, states that the People's Liberation Army must develop the necessary capabilities to wage a "*local war under informationisation conditions*", changing the previous review in 1993, which stipulated the wage of a "*local war using cutting-edge technology*". As it can be seen, the modification includes the concept of *informationisation* to emphasise the importance of cyber domain and associated activities in the preparation and execution of military operations. As a result of this change of approach, the Chinese People's Liberation Army has set the target year 2050 to achieve complete *informationisation*.

² Sun Microsystems Fined \$291,000 in Crackdown, <http://articles.latimes.com/2003/dec/16/business/fi-rup16.1>

Structures with responsibilities for cyber domain

There are no reliable data on the structures with responsibilities for cyber warfare and their missions related to cyber attacks or cyber protection. Based on the analysis of numerous public sources, it can be concluded that a series of structures are involved in cyber-related activities. They act to achieve the objectives set by the Chinese political and military decision makers.

Cyber attack and defence actions are performed by different structures inside the People's Liberation Army as well as by other structures outside the army³.

The 4th Department of the Chinese People's Liberation Army General Staff, formerly called the Department of Electronic Countermeasures, seems to have the key role in the execution of offensive information warfare. This department was established in 1990, with responsibilities for electronic warfare. Currently, the main responsibility of this structure is to perform information attack missions. The Department maintains authority over the army radio-electronic warfare regiments and uses, in the exercises it organises and conducts, both electronic countermeasures, specific to the above-mentioned regiments, and cyber warfare-associated capabilities.

The 3rd Department of the General Staff is intended mainly for SIGINT activities (intercepting communications and non-communications data). Moreover, this department has tasks related to data security of the Chinese People's Liberation Army voice and data networks. The 3rd Department has a monitoring centre that operates 24 hours a day and includes the Academy of Military Sciences, the National Defence University and three research institutes.

Some sources⁴ mention the existence of twelve operational bureaus, located in various regions of China, responsible for SIGINT data collection regarding targets of strategic relevance. They are believed to also act to protect own military networks, as well as to exploit computer networks in other countries.

The twelve bureaus are supposed to have the following domains of expertise and activity:

- 1st Bureau – has different specialised responsibilities;
- 2nd Bureau – is interested in the USA and Canada, being especially focused on information in the political, economic and military field;
- 3rd Bureau – has responsibilities for radio communications and border control networks;

³ *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf

⁴ *China's Cyber Capabilities*, <http://www.indiandefencereview.com/news/chinas-cyber-capabilities/>

- 4th Bureau – is responsible for Japan and the Republic of Korea;
- 5th Bureau – focuses on issues related to the Russian Federation;
- 6th Bureau – is involved in education and training activities;
- 7th Bureau – has responsibilities for computer networks defence and cyber attacks;
- 8th Bureau – focuses on Europe, Middle East, Africa and Latin America;
- 9th Bureau – provides strategic analysis regarding military intelligence and database management;
- 10th Bureau – also called 7911 Unit, has responsibilities for monitoring missiles, as well as for the nuclear tests in Central Asia and the Russian Federation;
- 11th Bureau – also called 2020 Unit – has also missions related to the Russian Federation, given the fact that it has experts in the Russian language;
- 12th Bureau – is probably involved in collecting data regarding satellite communications.

Besides the mentioned structures belonging to the army, there are cyber militia units destined for information warfare. These units are made up of IT professionals, operating within various companies throughout China, and have tasks related to cyber offensive and defence⁵.

The Ministry of Public Security provides active support in research on information security, certifying the products to be used by state institutions, including the army. The 3rd Institute of the Ministry of Public Security is responsible for creating security standards for the hardware and software components used in the military and government⁶.

It is considered that the new Chinese cyber capabilities and the abilities to use them in the context of a conflict generated by China (against Taiwan or another country in Asia) should be signs of serious concern to a state that would assess the possibility of its intervention to protect a certain entity assaulted by China.

Chinese military analysts identify the US C4ISR and logistics infrastructure as the centre of gravity of the US military strategy. Based on the above-mentioned findings, it is easy to understand that this conceptual element is applied to any other state and it represents a milestone for the Chinese leadership

⁵ Jeffrey Carr, *Inside Cyber Warfare*, second edition, O'Reilly Media, Inc., 2012, p. 257.

⁶ *Chinese Capabilities for Computer Network Operations and Cyber Espionage*, http://www.washingtonpost.com/r/2010-2019/WashingtonPost/2012/03/08/National-Security/Graphics/USCC_Report_Chinese_Capabilities_for_Computer_Network_Operations_and_Cyber_%20Espionage.pdf

with regard to what key components in cyber domain mean, which are important to the cyber-specialised Chinese military forces in the event of a conflict⁷.

The military strategist Sun Tzu's philosophy continues to have an important influence on the Chinese military strategic thinking. For example, Colonel Wang Baocun, a cyber warfare expert of the Chinese People's Liberation Army, states that cyber warfare is a very good example of Sun Tzu's assertion regarding "to subdue the enemy without fighting". He has also said that cyber attacks can be used to change the perceptions and beliefs of the opponent, and to make him give up the desire to fight⁸.

Cyber warriors training

"Cyber warriors" training is performed in several educational institutions, where there is professional staff specialised in different areas of the cyber domain. The main training centres for the Chinese People's Liberation Army cyber specialists are: the Communications Command Academy in Wuhan, Zhengzhou University of Information Engineering, the University of Science and Technology, and the National University of Defence Technology in Changsha. The courses attended by Chinese officers focus on computer networks technology, electronic countermeasures, radar technology, cyber warfare rules and strategies, information systems, information weapons, information systems protection, jamming and protection against jamming etc⁹.

*

The Chinese People's Liberation Army pays special attention to cyber domain, concluding partnerships with different private companies working in the IT field not only to maintain a high level as far as the technology used is concerned but also to have access to cutting-edge technology.

The new possibilities offered by the development of cyberspace have resulted in establishing structures dedicated to information warfare with responsibilities for cyber warfare as well as in remodelling existing structures. In this way, China intends to stand out and remain among top states in terms of possession and use of cutting-edge cyber capabilities.

English version by

 **Diana Cristiana LUPU**

⁷ *Idem*, http://www.washingtonpost.com/r/2010-2019/WashingtonPost/2012/03/08/National-Security/Graphics/USCC_Report_Chinese_Capabilities_for_Computer_Network_Operations_and_Cyber_%20Espionage.pdf

⁸ *Cyber Warfare. An Analysis of the Means and Motivations of Selected Nation States*, <http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf>

⁹ *Ibidem*.

SECURITY STRATEGIES IN CERTAIN EU MEMBER STATES – THE CASE OF SPAIN –

Dr Tiberiu TĂNASE

National Strategic Framework in the Field of Security and Defence

The emergence of new risks and threats to security, the implications of globalisation and the increasingly complex nature of modern conflicts have raised the need for the establishment of a Spanish security and defence system capable of responding efficiently to these challenges and protecting national interests. To accomplish this, it is mandatory for all instruments and resources available on a global scale to be integrated and harmonised.

In this article, the author presents Spain's intelligence community and its role in providing national security. In this respect, he describes the attributions of the three bodies of the intelligence community: National Antiterrorism Coordination Centre, National Intelligence Centre and Government Delegated Committee for Intelligence Affairs.

Keywords: *Spanish defence system; National Security Strategy; National Defence Directive; Islamic terrorism; human resources*

The field of security and defence has gone through important changes during the past years. The emergence of new risks and threats, materialised in the tragic attacks in March 2004, the implication of globalisation and the increased complexity of conflicts have determined the need for defining a Spanish security and defence system capable of efficiently meeting these requirements, pursuing national interests. In this respect, it is mandatory that all the instruments and resources available at national level are integrated and harmonised, an unitary action of the state in this field being thus provided.

After defining the *Defence White Paper*, in 2000, the first step in this respect was the *National Defence Directive 1/2004*, which enhanced the general concept of *strategic defence review*, from 2003, and brought about changes regarding the development of Spain's security and defence policy.

Consequently, the *Organic Law on National Defence 5/2005* highlighted Spain's importance

Dr Tiberiu Tănase – Lecturer at “Mihai Viteazul” National Intelligence Academy.

at national level, as well as its foreign policy, making the head of the government in charge of the direction of security policy, the development of its objectives and the drafting of the National Defence Directive. The Directive will have to be part of a *national security strategy*, whose necessity is obvious and which integrates the values and interests it is based on, at the same time analysing the risks, threats and vulnerabilities, as well as their causes, setting the framework of action and containing data for a proper response that should guarantee the protection of national interests.

This task given to the head of the government is in keeping with the general tendencies in the partner and allied states, a tendency that is aimed at integrating the objectives regarding each sector policy in a single national policy, at the same time providing the necessary coherence and coordination. Moreover, one must underline that concretely adapting to the evolution of the situation must be ensured by periodical strategic reviews. In the absence of a security strategy, the *National Defence Directive 01/2008*¹ is an important, new element that stresses the need for coordination among state actors, in an integrated perspective, in terms of security, as well as the compulsoriness of a strategic pyramid-like model.

The objective of the Directive is to set the guiding principles of the defence policy and the guidelines for its implementation, with dual purpose: providing national security and defence and contributing to maintaining international security and peace.

The current security environment is marked by profound changes in key areas of social existence. Globalisation makes notable progress, and current conflicts are defined by a multidimensional configuration. This multidimensional configuration of conflicts was created at the same time with the number of actors involved, either public and private ones, governmental and non-governmental, in conjunction with the economic, cultural, ethnic or religious ones, whose degree of intervention is variable in space and time.

To the traditional risks and threats to security, which involve an exclusively military liability, one may add others, which contribute to the degradation of social and economic development of countries and regions, with negative consequences both at national and at international level. In this respect, terrorism, organised crime and proliferation of weapons of mass destruction are the main transnational threats to the Spanish society. The hypothesis of their combination will definitely have devastating consequences. The 9/11 2001 attacks in the United States,

¹ At www.mde.es/documentacion/centroDocumentacion; this document describes the current security environment, as well as the risks and threats to Spain's security.

those on 11 March 2004 in Spain and on 7 July in the UK demonstrated the ability and motivation of terrorist groups.

The struggle for access to basic resources will be one of the main sources of conflict. On the one hand, economic growth and population size of some emerging countries lie at the basis of the competition for the use of resources, energy sources, water. On the other hand, economic development causes imbalances that have negative effects internationally.

The action of man on the environment determines the emergence of new phenomena, climate change that may cause serious natural phenomena. Finally, the technological revolution, the “*information age*” determine a new dimension in Spain’s security and defence.

National Defence Directive 1/2008 also emphasises the role that Spain plays on the international stage. As a UN member, Spain is committed in multiple ways to ensuring international security and peace, actively participating in peacekeeping, crisis management and conflict resolution operations under the aegis of the Security Council.

Because national security is intrinsically linked to the security of Europe, Spain maintains a strong European security and defence policy, but that does not affect the transatlantic relationship structurally, NATO further ensuring the collective defence of its members. Thus, the ultimate objective of a European defence developed by the European Union should be organised around the transatlantic relationship, as the Alliance defines the military capabilities adequate to meet the new international context in the field of security and defence.

Spain’s security is interdependent with the security of the Mediterranean area, with a special relationship with Latin America, continuing to heavily promote bilateral, regional and multilateral relations in the field of the defence and security policy.

At the same time, globalisation causes the emergence of problem areas. Both the sub-Saharan region and the Asia-Pacific region require a major effort of the international community for pacification and stabilisation. At national level, the armed forces must have an adequate intervention and response capacity to ensure Spain’s security. At the same time, there is an increased demand from the Spanish society for an effective response of public administrations when confronted with emergency situations, catastrophes.

The Principles of Spain’s Defence and Security

The values of any country, Spain included, are sovereignty, territorial integrity, respect for the constitution, freedom, life and prosperity of its citizens. In the current international context, the protection of these values is not limited to the national territory, it goes beyond it. Thus, ensuring a stable international

framework, of peace, security and human rights observance, is a fundamental objective of Spain's defence policy. It should be emphasised, in this regard, the importance of respecting human rights, the legality and legitimacy by relevant national bodies and international ones that Spain is part of, for instance the UN.

Security and defence are guaranteed powers of the state, which are achieved by combining various instruments and policies. Thus, they are not the exclusive responsibility of the ministry of defence, but require a multidisciplinary approach and an integrated action of public administration structures in the field, as well as the convergence of civil, military, public and private instruments.

In this context, security and defence need own means and resources with a high degree of training, coordination and availability, capable of an effective, prompt response, and if necessary, of autonomous action to ensure national interests. At the same time, collective defence and security, with partners and allies, contribute to carrying out this objective, as well as to providing peace and international security.

Courses of Action for Spain's Defence Policy

➤ The courses of action are aimed at *ensuring security and defence* and implementing this goal through a systematic corroboration and an integration of all its information, prevention, deterrence, intervention and international cooperation resources, as well as through crisis situation management.

In this respect, there is a need for a permanent information of the parliament on issues related to national defence and use of armed forces in foreign missions, according to the established legal framework; support for the National Defence Council as coordinating, advisory body as well as for consultation of the head of government in terms of defence; promotion of a culture of security and defence in society, providing a better understanding of the Constitution and better support from the citizens of the armed forces.

➤ Another course of action refers to *Spain's engagement to maintain international peace and security* and is based on respecting international law and exercising the policy of multilateralism² as a concerted means of action in international relations, with the purpose of solving conflicts.

➤ *Increased solidarity with partners and allies* in terms of collective defence and regional security is another course of action, just as important.

² Commercial policy that requires that each country should keep a global balance between it and the countries with which it has commercial relations, according to Niță Dobrotă, *Dicționar de economie*, Editura Economica, 1999.

Considering these issues, defence policy is aimed at:

- Spain's contribution in the UN Security Council for the international defence, peace and security through a substantial contribution to peace support and humanitarian assistance missions carried out by it;
- strengthening CESDP, through cooperation in initiatives in this area, including aspects of intelligence, training and defence industry;
- support for NATO transformation process, providing the necessary capabilities to meet the new risks and threats, stressing the importance of collaboration with other international organisations, according to the principles and values of the UN Charter;
- intensifying diplomatic actions in the field of defence and cooperation with neighbouring countries and those in areas of strategic interest for Spain, while ensuring a strong and balanced relationship of cooperation with the United States;
- enhancing bilateral and multilateral relations with Latin America in terms of defence, encouraging the joint participation in peacekeeping operations, strengthening military cooperation in all fields, working to reform and modernise the security and defence sector;
- contributing, in the field of defence, to peacekeeping, recovery, stability of the African continent, the sub-Saharan region;
- collaborating and supporting the international community effort to stabilise and rebuild the Asia-Pacific region and, in particular, to establish a security environment in Afghanistan within the ISAF mission.

➤ *Obtaining a high level of social and political support* will enable the defence policy to be a genuine state policy, emphasising the need to promote a culture of security and defence in society, providing a better understanding of the Constitution and better support for the armed forces on the part of the citizens.

➤ *Dynamic and permanent transformation of the armed forces* and their adaptation to the new strategic framework will be essential elements of the national defence policy. In this respect, adapting their structures to the new model of inter-arms action will be achieved through: consistent and stable budgetary effort, professionalisation of existing branches, fostering research, development and innovation in the Spanish defence industry.

Despite these provisions, the European experience has shown that we need strategies tailored to meet the new security environment, characterised by uncertainty (*figure 1*). It is an environment in which European governments are increasingly interconnected, in which the changes in the system are spreading unpredictably and often chaotically: "*Cause and effect are no longer close in time and space*"³.

³ C. Edwards and S. Parker, *Futures Thinking and How to Do It*, Demos, 2008.

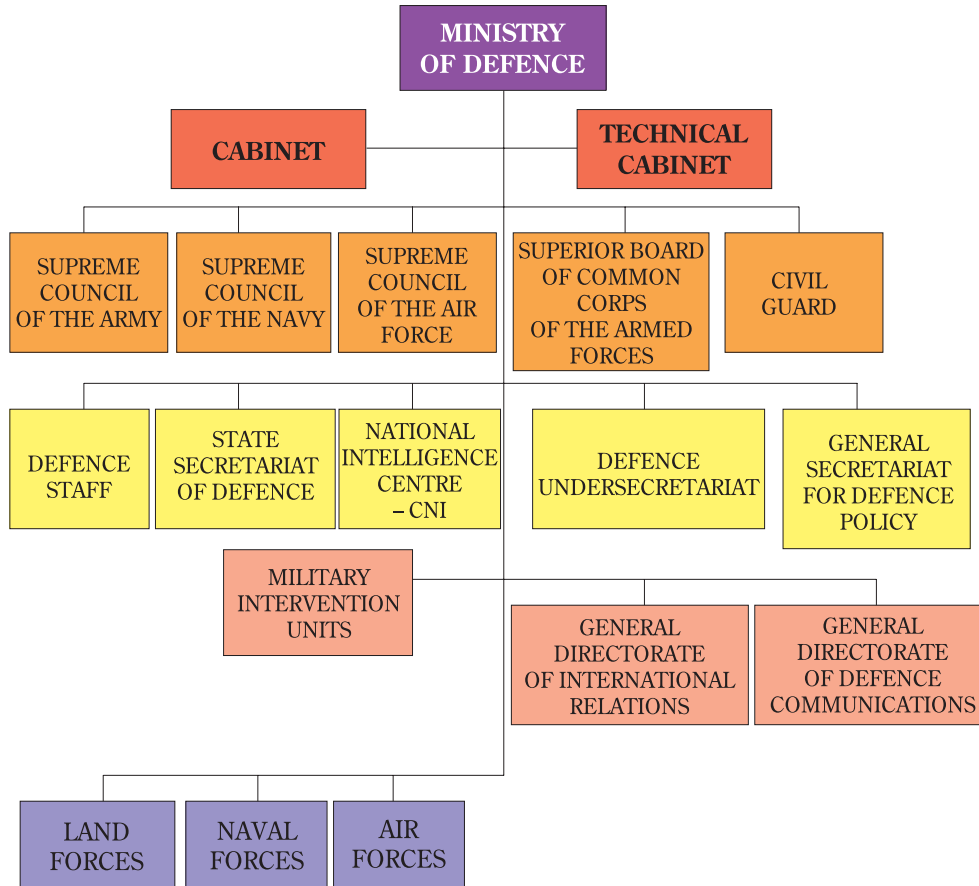


Figure 1: Spanish Defence and Security Structure*

Redefining the concept of *national security* expresses a necessity, considering that the risks and threats to Spanish national security are high. They are becoming increasingly interconnected, such as terrorism and organised crime. Thus, first of all, this strategic document will have to pursue the development of a global vision on the current and future security environment. Secondly, a security strategy aims to determine the awareness of the level of risks and, therefore, the granting of priorities. Regarding the allocation of funds and budgetary resources necessary, developing a governmental framework would ensure the synergy between the departments and agencies involved, developing the Spanish government's ability to anticipate the threats and challenges to the security of the society.

* According to www.mde.es.

In this respect, the *Security Strategy* plays an important role in: *defining national security interests; evaluating national and international security environment; identifying risk factors at national and international level; setting goals and objectives of defence policy, at national and international level; identifying courses of action and means to ensure national security.*

A third argument for the development of a new security strategy would be the need to adapt to the security strategies of international organisations (EU, UN, NATO, OSCE). Considering these aspects, the Spanish government should adopt a “*network*” approach to ensure national security; this will lead to greater interdependence between national security and intelligence departments and agencies.

Spain’s Intelligence Community and its Role in Ensuring Security according to the National Defence Directive

The Spanish Intelligence Community has three components:

- the actual intelligence structure, composed of the *National Antiterrorism Coordination Centre (Centro Nacional de Coordinacion Antiterrorista/CNCA)*, the *National Intelligence Centre (Centro Nacional Inteligencia/CNI)* and the Government Delegated Committee for Intelligence Affairs (*Comision Delegada del Gobierno Para Asuntos de Inteligencia/CDGAI*);
- military intelligence directorates, as well as departments for fighting organised crime.

❖ *National Antiterrorism Coordination Centre*

The centre was established on 28 May 2004. This permanent structure includes staff from the *National Police Force* and the *Civil Guard* (Guardia Civil), also benefiting from the support of about five agencies from the *National Intelligence Centre*. CNCA aims to collect, analyse and use all information regarding terrorist activities that are threats to national and international security.

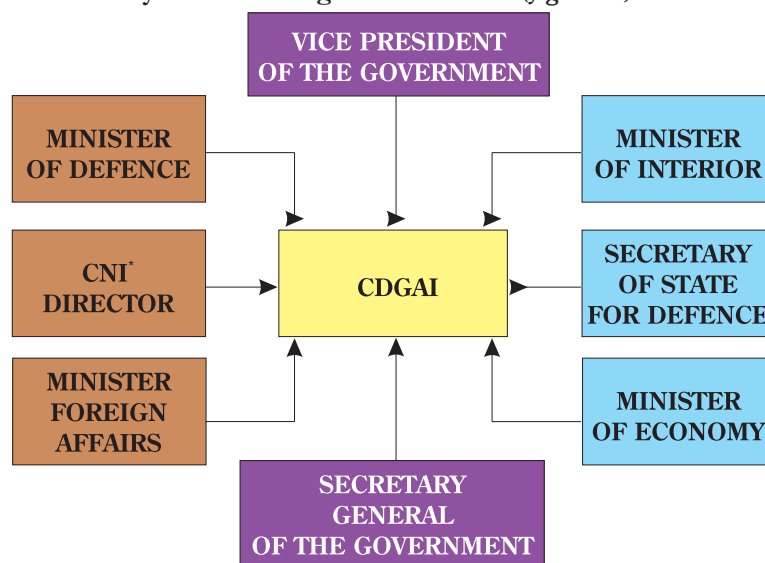
In this respect, CNCA has the following objectives: terrorist threats upgrading, countering terrorism initiative, identification of possible scenarios for action in combating terrorism and their planning, development of critical infrastructure list. CNCA reports directly to the Secretary of State for Security and the leadership of the Centre belongs, on a rotation principle, every two years, to the National Police and the Civil Guard.

❖ *National Intelligence Centre*

Following the 2002 reform, Spain’s main intelligence service became the *National Intelligence Centre*. Thus, Law 11/2002 of 6 May regulates the aims, principles,

legal framework of CNI and Law 2/2002, dated 7 May, regulates aspects regarding the control over its activity. Subsequently, Royal Decree 436/2002 of 10 May establishes the structure of CNI. The Centre is subordinated to the Ministry of Defence, but has in fact a functional autonomous status in terms of its internal organisation, budget and staff management⁴.

From the administrative point of view, CNI is headed by a director who has the rank of secretary of state. The CNI Director is appointed by royal decree, at the proposal of the Minister of Defence, for five years. CNI objectives are defined annually in the Intelligence Directive (*figure 2*).



* Commission Secretary

Figure 2

❖ By the development of the *National Intelligence Directive* by the **Government Delegated Committee for Intelligence Affairs** it is identified the need for the beneficiary regarding security information. The operationalisation of these objectives, basically, operational planning, is done according to a “*Permanent Intelligence Plan*”. Spain’s strategic particularities lead to the identification and classification of the priorities of intelligence services activities. Thus, the main goal of CNI is to provide the government with pieces of information in order to prevent and, if necessary, to eliminate all the risks and threats that affect Spain’s independence and integrity, national interests, stability of the rule of law and its institutions.

⁴ In 2008, it consisted of approximately 2 250 agents; in 2009, the budget of CNI was of 255 million Euros. CNI carries out activities in 80 countries, especially North Africa (it oversees the enclaves Ceuta and Melilla), in the Middle East and in North America, at http://www.mde.es/Organigrama/org_ministro_de_defensa.html.

CNI functions are regulated by Article 4 of Law 11/2002, as follows:

- to collect, analyse, exploit information for national security and for promoting political, economic, industrial, commercial and strategic interests of Spain;
- to prevent, detect and eliminate the activities of foreign services or groups of people that endanger constitutional order, rights and freedom of citizens of Spanish citizens, the sovereignty, integrity and security of the state, the stability of its institutions, its national economic interests and welfare of population;
- to promote cooperation and collaboration relations with intelligence services of other countries or with international bodies, in order to successfully meet the set objectives;
- to ensure information security through the National Cryptologic Centre (CCN), integrated into the CNI; this structure forms, certifies and accredits own personnel;
- to ensure technological and information security of various public administration bodies;
- to protect classified information – the National Security Office is the structure of CNI capable of protecting classified information;
- to ensure the protection of personnel and own infrastructure.

To achieve these functions, the areas of action of CNI are: *foreign intelligence; counter-terrorism; economy and technology; counterintelligence; information security; classified documents security.*

CNI structure – Royal Decree 432/2002, May 2002, and Royal Decree 612/2006, of 19 May, regulate the structure of CNI, which, in order to achieve greater efficiency in fulfilling its duties, is structured as follows: *Directorship, General Secretariat, Technical Directorates.*

The *Director* has the rank of Secretary of State and is appointed by Royal Decree on the proposal of the Minister of Defence. Its tasks are aimed: to develop the proposal regarding the organic structure of CNI; to establish cooperation relations, regarding the CNI activity, with intelligence services of the armed forces and of the security structures of the state, as well as with public administration structures in order to achieve the set objectives; to coordinate the activity of the *National Cryptologic Centre*; to coordinate the activity of the *Delegated National Security Authority (Autoridad Nacional de Seguridad Delegada/ANS-D)*, whose mission is to provide NATO and EU classified information management.

The *General Secretariat* is headed by a Secretary General who has the rank of Under Secretary of State, appointed by Royal Decree, on the proposal of the Minister of Defence. Its functions are: to help and support the Director

in activities; to establish mechanisms and organisation systems of the National Intelligence Centre and to determine precise actions to update and improve them; CNI personnel management.

Technical Directorates:

➤ *Technical Intelligence Directorate*, which is in charge of the following sub-directorates:

1. *Foreign Intelligence Sub-Directorate*, responsible for obtaining, evaluating and disseminating information in order to prevent the dangers, threats to or external aggression against Spain's independence or territorial integrity, ensuring national interests.
2. *Counterintelligence Sub-Directorate*, whose duties are to detect and neutralise the activities of foreign intelligence services in Spain.
3. *Counterterrorism Sub-Directorate* replaces the old *Domestic Intelligence Division* and assumes the functions stipulated by Law 4/2002, as follows: prevention, detection and possible neutralisation of groups or persons causing risks, threats or attacks against the constitutional order, rights and freedoms of Spanish citizens, the sovereignty, integration and security of the state, the stability of institutions, economic interests and the rule of law; coordination of the activity with the other structures specialised in fighting terrorism, especially with the *National Antiterrorism Coordination Centre*.
4. *Technical Sub-Directorate* is responsible for obtaining, evaluating and intercepting strategic signals traffic; for legally intercepting communications, interpreting images intercepted by satellites.
5. *Operative Intervention Sub-Directorate*.

➤ *Technical Directorate of Support in the Intelligence Activity* must accomplish operative missions, using adequate equipment and means to obtain information.

➤ *Technical Resource Directorate* is in charge of the following structures: *administrative department, financial department, personnel management department, training centres. Training centres are in charge of training the personnel of the National Intelligence Centre, organising personnel training and improvement courses in the technical, communications, intelligence analysis, foreign languages fields as well as training personnel for missions abroad.* In this respect, the functions of training centres are: to develop courses necessary for staff training and improvement courses in line with the objectives of CNI or in keeping with collaboration conventions, with similar structures or services; to set up schedules, courses, seminars and any other activities for training and specialising the personnel of the National Intelligence Centre.

Supporting structures of the Secretary of State-Director are the *Offices of the Secretary of State-Director* and the *Legal Consultancy*.

Integrated structures of CNI are: *National Cryptologic Centre*, *National Security Office (Oficina Nacional de Seguridad/ONS)*, *National Intelligence and Counterintelligence Office (Oficina Nacional de Inteligencia y Contrainteligencia/ONIC)*.

National Cryptologic Centre's mission is to coordinate the different structures using cryptologic procedures and to ensure the security of information technology.

National Security Office, created in 1983, is integrated into the security division of CNI, its function being to ensure security of NATO/EU classified information. At the same time, ONS manages the access to NATO/EU classified information and ensures the management of classified information concerning bilateral and multilateral agreements regarding defence industry.

National Intelligence and Counterintelligence Office's mission is to coordinate the activity of the National Intelligence Centre, developing and maintaining cooperation between the intelligence structures and the other security structures, as well as with state institutions in order to achieve objectives.

The main beneficiaries of the final product of CNI (security information) are: the Prime Minister, ministries (Ministry of Foreign Affairs and Cooperation, Ministry of Defence and Ministry of Interior) and other departments of state administration. CNI is a structure that supports, through reports, the decision-making process, being responsible for actions taken based on these reports. All information that regards the activity of CNI, its organisation, internal structure, means and procedures, personnel, technical resources, database, information sources is classified and top secret, in accordance with specific legislation and international agreements.

As far as parliamentary control is concerned, CNI provides the Congress of Deputies, in keeping with its regulations, through the Parliamentary Committee, responsible for budget control and led by Congress President, with information on its activity. The reunion of the Committee and the communicated information are secret.

Legal control is provided by a magistrate of the Supreme Court, appointed by qualified majority by the General Council of the Judiciary. He must give his consent in respect of all measures that result in violation of residence or postal secrecy, on condition that such measures are included in the tasks and functions of the CNI.

Analysing the presented issues, we can say that intelligence services reform produced significant changes, the structures becoming more flexible

and the intelligence components being coupled with the counterintelligence one in a more efficient way.

Nevertheless, the attacks that took place in Madrid on 11 March 2004 took the *National Intelligence Centre* and even the antiterrorist coalition by surprise, demonstrating that there is neither panacea nor easy solution in combating terrorism.

In fact, the Madrid 2004 event was followed by a series of important steps, among which:

- ratifying a package of measures to support the fight against Islamic terrorism, which covers a wide range of issues, such as checks on delivered funds and money transferred electronically, in order to avoid situations where charities are used as a source of terrorist financing, as well as increasing the controls at the Bank of Spain to identify holders of financial products considered to be “*potentially dangerous to national security*”;
- hiring agents and translators in units dealing with the fight against Islamist terrorism. In parallel, the leadership of the National Intelligence Centre launched a broad campaign to recruit new agents, especially ones who know classical Arabic language or its dialects or Chinese etc.

*

Taking the example of France and Great Britain, Spain needs a new security strategy that meets the 21st century challenges. Undoubtedly, a Spanish national security strategy is the appropriate response to the uncertainty and complexity of the current and future security environment, which is something recognised at the level of member states. Moreover, developing a national security strategy with a clear focus on intelligence must be regarded as the most effective investment for the future.

The 21st century is marked by profound changes in the international security environment. The world becomes increasingly complex and interdependent, and the phenomenon of globalisation is irreversible. The emergence of a global economy, strongly interconnected, reconfigures the system of international alliances, accelerates the adoption of technologies and broadens the development of new economic centres. This interconnected world offers new opportunities, but develops significant risk to international security.


Regional instability, resulting from the spread of religious fundamentalism, massive migrations of populations and competition for natural resources, among other factors, are the coordinates that define new requirements for intelligence and security services.

The concerns of states for organising more effectively intelligence services have increased in recent years and especially after the terrorist attacks

in the United States and Europe. Intelligence services must help reduce international risks and threats to the country by participating in the effort to achieve information superiority in certain areas of interest. When general objectives are articulated in a national strategy, specialised information services and agencies programmatically subordinate their entire activity to the way in which national goals are translated into intelligence missions. It is a general, systematic and long-term approach, which must take place in the entire national intelligence system for it to meet the expectations regarding the protection of national interests.

BIBLIOGRAPHY

1. Charlie Edwards, *Spain in the 21st Century: The Case for a National Security Strategy*, Real Instituto Elcano, 2008.
2. Antonio M. Diaz Fernandez, *Los servicios de inteligencia españoles. Desde la guerra civil hasta el 11-M. Historia de una transición*, Madrid, Alianza Editorial, 2006.
3. Antonio Fonfria Mesa (coord.), *Hacia Una Estrategia de Seguridad Nacional Para España*, Centro Superior de Estudios de la Defensa Nacional, 2009.
4. Tiberiu Tănase, Ana Maria Porumbiță, *Considerații privind transformările și adaptarea serviciilor de informații și securitate la noul mediu de securitate al secolului al XXI-lea*, *Stabilitate și Securitate Națională*, UNAp, April 2008.
5. *Spain's Intelligence Community and its Role in Providing National Security*, www.cni.es, www.mds.es; *Libro Blanco de la Defensa*, MDE, Madrid, 2000.
6. www.cni.es.
7. www.nids.es.

English version by
 **Iulia NĂSTASIE**



NATO Enlargement Reloaded

Karl-Heinz KAMP

In this article, the author addresses the issue of NATO enlargement, expanding upon it with examples such as FYROM, and the name-dispute that did not allow it to become NATO member despite being ready to join NATO as early as 2009, Montenegro, with significant progress, Bosnia-Herzegovina, and the conditions attached for joining the Alliance, Georgia, elaborating on the pros and cons of Georgian NATO membership, Ukraine, with a large pro-Russian population in its Eastern part and with particular historical significance for Moscow.

Then, he writes about the roots of the delicate membership debate and about Russia's perspective on NATO admitting new members from the former Eastern hemisphere, during the almost twenty years of the enlargement process.

To conclude, the author gives us his insight into how to deal with the membership question with regard to the four aspirant countries: Bosnia-Herzegovina, FYROM, Georgia and Montenegro.

Keywords: *NATO enlargement; Russia; FYROM; Georgia; Cold War; Bosnia-Herzegovina; Montenegro*

The dispute about *who* will become a new NATO member and *when* is set to make it back on the transatlantic agenda. Debates in the Alliance have for years been dominated by the operations in Afghanistan or the evolution of NATO's partnership approach, but now the enlargement question is coming up again and might lead to strong disagreements among the allies. All NATO nations certainly concur that the door for new members should remain open; the question is which countries should join the Alliance, and when?

At NATO's Chicago Summit in May 2012, US Foreign Secretary Hillary Clinton suggested that Chicago should be the last NATO summit not explicitly focusing on enlargement¹. From this statement, which went largely unnoticed by the public, it can be logically inferred

The article was featured in the *Research Paper* no. 81, September 2012, of the NATO Defense College, Rome, <http://www.ndc.nato.int/research/series.php?icode=1>.

Karl-Heinz Kamp is the Director of the Research Division at the NATO Defense College. The views expressed in this paper are the responsibility of the author and do not necessarily reflect the opinions of the NATO Defense College or the North Atlantic Treaty Organisation.

¹ At the Atlantic Council meeting on 21 May, Foreign Secretary Clinton stated: "... *I believe this summit should be the last summit that is not an enlargement summit*". See <http://www.state.gov/secretary/rm/2012/05/190466.htm>

that *all* forthcoming summits should deal with inviting new members to join NATO, showing the degree of emphasis the US government is set to place on the enlargement issue in the coming years. Even if a statement of this kind in Chicago – in the midst of the presidential campaign and at the first NATO summit on US territory since 1999 – is partly directed to a domestic audience, it still shows the current mood in US political circles: NATO enlargement is regarded as a unique benefit, and the United States sees itself as the spearhead of the movement in favour of this.

With regard to most countries currently applying for NATO membership, the issue is hardly controversial within the Alliance². The Former Yugoslav Republic of Macedonia (FYROM)³ was ready to join NATO as early as 2009, together with Albania and Croatia. An almost bizarre dispute about the name of the country led Greece to veto FYROM's accession and keeps it still pending. Other allies, particularly the United States, are becoming increasingly impatient with the Greek obstructionism on this question. In March 2012, 54 members of the US Congress sent a letter to President Obama pressing for timely admission of FYROM. The FYROM case is thus more a procedural issue, and not a dispute on a "yes" or "no" to membership. The very moment Athens lifts its blockade, FYROM can become a member immediately.

Montenegro was admitted to NATO's *Membership Action Plan (MAP)* in December 2009, and is said to have progressed significantly in meeting membership requirements since then. Bosnia-Herzegovina was invited to join the MAP in April 2010, albeit with certain conditions attached. According to those in favour of their accession, both these relatively small countries deserve an invitation to join NATO in the near future. This holds all the more true as their integration into Alliance structures would not pose insurmountable problems and, by contrast with such cases as the (former) application of Ukraine, should not stir up Russian protest.

The crunch point of the enlargement question, however, is Georgia, a country that was involved in a war with Russia and still has Russian occupation forces on its territory in the renegade regions of Abkhazia and South Ossetia. In 2008, the George W. Bush administration was pushing strongly for Georgia and Ukraine to join NATO – in the case of Georgia, despite (or because of) its dispute with Russia – whereas Germany, France and many others were opposed to rapid admission of these two countries. The case was settled with a compromise, and hardly anything more has been done on it since then. Now, after a long,

² In December 2011, NATO defined Georgia, FYROM, Montenegro and Bosnia-Herzegovina as "*aspirant countries*" and gave particular recognition to their interest in membership.

³ Turkey recognises the Republic of Macedonia with its constitutional name.

undeclared “*cease-fire*” within the Alliance over enlargement, the upcoming revival of the debate is set to bring the Georgia issue to the fore again. However, the battle order has in the meantime apparently changed to a significant degree. In particular, informal discussions within the Alliance in mid-2012 showed that Washington heads a large majority of NATO members in favour of enlargement (including Georgia), whereas Germany and only a few others still strongly oppose such a step.

This paper evaluates what is at stake in the newly emerging enlargement debate. What are the pros and cons of Georgian NATO membership, and how should the Alliance proceed?

Two Difficult Membership Applicants

The dispute over Georgian membership within NATO dates back to the Bucharest Summit in April 2008. Georgia was one of the first to sign NATO’s Partnership for Peace (PfP) programme in 1994, and always justified its strong desire to join the Alliance with what it perceived as the threat emanating from Russia. In 2008, according to Georgian polls, 77% of the public supported a referendum on NATO membership. In the weeks prior to the summit, Georgia as well as Ukraine strengthened their demands for membership, the immediate goal being admission to the MAP. In NATO, there was a tacit consensus to keep the door for both countries open, but at the time it was felt that it was still premature to take them into the MAP.

At the summit, President George W. Bush surprisingly started touting again for rapid NATO membership for both countries. Many allies were highly skeptical with regard to the wisdom of such a step. Ukraine is the second largest country in Europe (after Russia), with a large pro-Russian population in its Eastern part and with particular historical significance for Moscow. Its integration into NATO did not seem feasible, and could have led to fierce Russian protest, probably ending NATO-Russia cooperation once and for all. While Georgia would have been a much smaller bite to digest, it was already engaged in a long smouldering conflict with Russia over its renegade regions (Russia had shot down a Georgian drone over Abkhazia). There was thus general concern that the escalation of the conflict could drag NATO into an Article 5 situation if Georgia were to become a NATO member.

In Bucharest, NATO reached consensus by not taking Georgia and Ukraine into the MAP, but giving both countries an explicit promise that they would be admitted to the Alliance. The Summit declaration stated: “*We agreed today that these countries will become members of NATO*”⁴, without specifying a concrete date for admission.

⁴http://www.nato.int/cps/en/natolive/official_texts_8443.htm

Another important step at this time was the foundation of the NATO-Georgia Commission, in addition to the already existing NATO-Russia Council and NATO-Ukraine Commission, in order to emphasise the special status of Georgia in comparison to other applicant countries.

In the short term, this settlement appeased all sides – albeit with a price to pay, in that NATO gave up a core principle of its enlargement policy since the mid-1990s: taking in new members on an individual basis according to their merits, which have to be proved in a gradual and transparent process. The Bucharest statement, instead, gave a *guarantee* for membership (sooner or later), without referring to merits or prior achievements. This was one of the many “*falls from grace*” in the entire enlargement process – politically necessary at the time, but sowing the seeds for later trouble and inconsistencies.

Months later, in August 2008, the Russian-Georgian war started and was immediately used as grounds for arguing in favour of or against rapid NATO membership for Georgia. Those in favour argued that Moscow would not have dared wage military action against Georgia if the country had already been a member of the Alliance. Opponents of Georgian membership pointed to the difficult situation for Alliance if one of its members were to be involved in a war with Russia.

In the meantime, the other “*difficult*” NATO applicant (Ukraine) indicated that it was no longer interested in speedy admission to the Alliance. In June 2010, the Ukrainian parliament adopted a law declaring that the country would pursue a non-bloc policy, i.e. it would not participate in political-military alliances but would further develop its partnership with NATO from a non-aligned position⁵. Hence, it is Georgia which remains the major stumbling block in the upcoming enlargement debate.

The Roots of the Debate

Since the end of the East-West conflict, the question of whether or not to accept new members in NATO has been highly disputed. Supporters at the time pointed to the benefits new members could bring to NATO, while skeptics warned against the repercussions on the relationship with Russia or pointed to the difficulties of finding consensus in an ever-growing Atlantic Alliance. Particularly in Germany, one of the driving forces in the first enlargement round after the Cold War, some wanted to limit the enlargement process to a very small number of states: the argument for this was that NATO should prove its capability to enlarge,

⁵ <http://euobserver.com/13/30212>

but should neither overstretch its capacity to integrate new members nor fuel Russian concerns about a constantly growing Alliance. By this logic it was thought that Hungary, Poland and the Czech Republic should be admitted, whereas the Baltic States – sharing common borders with Russia – should be kept out for as long as possible.

This approach quickly proved to be illusory, since more and more countries applied. NATO therefore needed criteria by which to assess the growing number of candidates. What should be the merits and achievements according to which a membership application should be granted? Unfortunately, the need for clear membership benchmarks was at odds with NATO's traditional reluctance to have its freedom of action limited by fixed and formal standards. NATO allies understandably did not want to find themselves in a situation where they had to accept an applicant country which fulfilled all the given norms and conditions but was not appreciated for other political reasons.

In addition, despite the overall consensus that NATO should pursue an open door policy, the motives of single NATO members for supporting individual applicant countries differed and evolved over time. Some NATO nations backed candidates in their immediate vicinity, in order to stabilise their neighbourhood. Others voted for aspirants in consideration of long-standing historical or cultural ties. Some supported countries which were not controversial from a Russian point of view, while others were in favour of applications from countries which were contentious for Moscow.

As a result, NATO conducted the entire enlargement process in a slightly twisted manner. In its *Enlargement Study* of September 1995, the Alliance defined a number of specific and transparent criteria for applicants to fulfil with a view to becoming members (and also to comply with after joining the Alliance). At the same time, decision-making processes in the three enlargement rounds since the end of the *Cold War* (1999, 2004, 2009) were strongly affected by political considerations which went beyond this set of rules and regulations. As a result, not all of the new members were fully in line with what the *Enlargement Study* stipulated, namely that enlargement should be a benefit not only for the admitted countries but also for the efficiency of NATO itself. Some of the 12 countries which have become members since 1999 swiftly neglected the promises they made prior to accession (like keeping their level of defence spending at 2% of Gross Domestic Product), and contribute appallingly little to NATO's overall capabilities. Others show worrisome levels of corruption and nepotism, which could even harm NATO's security standards – particularly with respect to classified information.

If the forthcoming NATO summits will all have to deal with the membership question and bring the enlargement debate into the limelight, then there is bound

to be further discussion of benchmarks and criteria. The *Enlargement Study* of 1995 can still function as a guiding document. However, given the experiences of the past, it is likely that NATO's decisions on enlargement will (again) not be taken solely on the basis of objective principles, but also according to political preferences or individual perceptions.

Russia and Enlargement

During the almost twenty years of the enlargement process⁶, Russia has vehemently opposed NATO admitting new members from the former Eastern hemisphere. For Moscow, NATO "*expansion*", as the Russians call it, is always a zero sum game: any new member for NATO means a loss of influence or power for Russia. This holds all the more true as, from Moscow's point of view, NATO is an institution which should in any case no longer exist. Russian reactions, particularly from military representatives, have at times been almost hysterical, with threats of military action against NATO (even nuclear strikes) in the event of membership being granted to, for instance, the Baltic States. It is safe to assume that such panic-stricken outbursts were in line with the political leadership in the Kremlin – a NATO General threatening the use of nuclear weapons against Russia would be fired within minutes. The idea that NATO enlargement de facto stabilised Russia's Western neighbourhood, which might otherwise have been exposed to regional crises, was never openly acknowledged by Russian military or political decision-making circles.

NATO, instead, emphasised its respect for Moscow's legitimate security interests. However, the Alliance never accepted any Russian veto against a country applying for membership. NATO was never actively campaigning for new members, but respected the desire of sovereign states to choose the alliance they want to belong to. Still, despite NATO's guiding principle of an open door policy toward potential new members, there were always different opinions within the Alliance as to how far Russian concerns should be taken into account. The position of core allies has, indeed, shifted considerably in this respect. When Germany brought up the idea of enlargement in 1993 the then US administration opposed any such proposal, not least because Deputy Secretary of State Strobe Talbot strongly argued in favour of a "*Russia first*" policy. In autumn 1994, the Clinton administration reversed its stance on membership, not least for domestic reasons (midterm elections), and became the prime supporter of enlargement. By the 2008 Bucharest Summit, the relative positions of the US and Germany had come full circle: the Bush administration

⁶ Arguably, the enlargement process began with the speech of German Defence Minister Volker Ruehe at the London-based *International Institute for Strategic Studies (IISS)* in March 1993.

was pushing for a membership signal to Ukraine and Georgia (not least as an anti-Russian move), whereas Germany led the group of those opposing this line so as not to alienate Russia.

Are-emerging debate on enlargement will certainly reawaken Russian protests and lead to open military threats, particularly if it comes to Georgia. How sensitive the issue still is for Russia can be seen in the then President Medvedev's November 2011 statement that one purpose served by the war with Georgia was that of stopping NATO enlargement in the region⁷. In addition, the continuing tendency to express military threats in response to unwelcome developments in NATO is seen in the May 2012 statement of the Russian Chief by the General Staff, General Makarov, regarding the use of pre-emptive strikes against NATO missile defence sites⁸.

However, despite Russian disapproval of future enlargement, Moscow's foreseeable threats will arguably ring hollow. On the international scene – and not only in the Middle East – Russia has lost much of its former influence. It is no coincidence that, in the recent Pentagon paper on US defence priorities for the 21st century, Russia is mentioned with only one generic sentence⁹. More importantly, with regard to its economic, military and societal modernisation, Russia has lost ground and is currently occupying an international position that lends no support to its pretensions of being at eye level with NATO. Russian resistance will keep NATO neither from building up a missile defence capability nor from inviting countries to join the Alliance if all 28 NATO nations approve.

At the same time, a future NATO member state which has Russian troops on its soil and is involved in an ongoing dispute with Moscow about the status of occupied territories would provide Moscow with a lever to negatively influence NATO's cohesion.

Georgia in NATO – Pros and Cons

A standard argument brought forward in favour of Georgian NATO membership is that of "*unfinished business*". While NATO leaders have constantly repeated their vision of a *Europe whole and free*, it seems obvious that the previous three enlargement rounds have omitted parts of Europe. To date, this claim

⁷ Denis Dyomkin, *Russia Says Georgia War Stopped NATO Expansion*, Reuters, 21 November 2011.

⁸ <http://www.nytimes.com/2012/05/04/world/europe/russian-general-threatens-pre-emptive-attacks-on-missile-defense-sites.html>

⁹ "*In addition, our engagement with Russia remains important, and we will continue to build a closer relationship in areas of mutual interest and encourage it to be a contributor across a broad range of issues*". Department of Defense, *Sustaining US Global Leadership: Priorities for 21st Century Defense*, Washington DC, January 2012.

has been brought forward mostly with reference to the Western Balkans, where some countries have already joined the Alliance in recent years whereas others like Bosnia-Herzegovina or Montenegro are still awaiting an invitation. Accepting these countries as members would mean – according to supporters of enlargement – exporting stability to the region via the Alliance’s unspoken code of conduct. Since NATO even went to war in 1999 to support stability in the Balkans, it seems obvious that it feels a particular responsibility for this part of Europe.

Initially, Georgia was not included in the “*unfinished business*” reasoning, as there was actually a dispute over whether the country even belongs geographically to Europe at all (Article 10 of the Washington Treaty makes provision for NATO membership only for European and North American countries). Since NATO’s Bucharest declaration guaranteeing Georgian membership, however, Georgia has been seen as a part of Europe (if not geographically, then certainly politically) and needs to be taken into the Alliance sooner or later. It is therefore hard to deny that the question of inviting Georgia to join is, indeed, part and parcel of the unfinished business.

A second argument brought forward in favour of Georgian membership is that the country has proved its readiness to contribute to NATO operations. In Afghanistan, Georgia has been one of the largest force providers in relation to the size of the country, and has suffered casualties. Even if Georgian soldiers received significant support in terms of equipment (to a large degree provided by Germany), providing more forces than some of NATO’s full members has been a noteworthy achievement. Given the international financial crisis and the expected budget cuts in all NATO countries, supporters of enlargement point to new members as a way of improving the Alliance’s overall capabilities. In this respect, Georgia’s relatively positive economic development offers solid grounds for seeing the country as a net provider of security, both with its current partner status and once it joins NATO.

On the negative side, two points seem crucial. First, complaints that the Chicago Summit made no progress with regard to the enlargement issue – something which also seems implicit in the statement of Secretary Clinton on NATO’s future summit agendas – need to be assessed critically. NATO enlargement is not a value in itself, and it is not the core function of the Alliance to admit new members. Instead, enlargement *can* strengthen NATO and should therefore occur only if it is a win-win situation for the applicants as well as for the Alliance. This does not necessarily mean that Georgian membership would not be good, but at the same time countries should not be invited with the sole purpose

of keeping the enlargement process going. A *Europe whole and free* is certainly NATO's long-term vision for the continent, but this does not imply that all European states must necessarily be members of the Alliance. In that sense, the 1995 *Enlargement Study* with its clear statements on the benefits enlargement has to bring for NATO is still seminal.

Second, it is not so much Russian dissent that requires caution in the enlargement question. Russia's protest will come by default, and cannot be the yardstick for NATO's decision-making on new members. The real underlying problem is that the territorial disputes between Russia and Georgia over the two renegade regions could lead to another war in the region. A military conflict between Russia and a Georgia with NATO member status would most likely lead to an Article 5 situation in which NATO would have to support Georgia and could find itself in a war with Russia. How credible would NATO's Article 5 commitment be under such circumstances? There are even concerns that a future Georgian leadership could feel tempted to behave more offensively vis-à-vis Moscow, knowing that in a conflict it would be backed by the North Atlantic Alliance. Admittedly, this "*mourir pour...*?" question was always present during the entire enlargement process: would 28 NATO members be prepared to go to war with Russia to protect, say, Tallinn or Riga? With regard to the credibility of US nuclear commitments for Europe, it was even relevant for the "*old*" NATO members throughout the *Cold War*: would the United States endanger San Francisco (by exposing it to Soviet nuclear retaliation) to protect Frankfurt, Amsterdam or Rome? Questions such as these can never be answered in advance, and will always depend on circumstances and on the specific situation. One can leave it to future debate to determine whether the lukewarm reaction of many NATO allies during the 2008 Russia-Georgia war makes it possible to draw any conclusions in this respect.

For good reasons, the *Enlargement Study* stipulates, in Article 6 of the document, that applicants with territorial disputes or irredentist claims need to settle them by peaceful means before they can join NATO. Also important is the more general provision in Article 10 of NATO's founding document, the *Washington Treaty* of 1949, to the effect that aspiring member states should be in a position "... *to contribute to the security of the North Atlantic area...*". In this respect, inviting Georgia to join before its territorial disputes are solved could import instability into NATO, rather than improve the overall performance of the Alliance.

Some supporters of rapid Georgian admission argue that NATO broke the principle of not importing territorial disputes even in its earliest history: in 1955 Germany was invited to join the Alliance, notwithstanding the fact that more than a third of its territory was occupied by the Soviet Union and that the communist "*German Democratic Republic*" was internationally

recognised only by a few states in the Eastern hemisphere. However, the overall situation at the beginning of the *Cold War* was fundamentally different and cannot be compared to the Georgian-Russian disputes over Abkhazia and South Ossetia.

How to Deal With the Membership Question?

It can thus be seen that the four aspirant countries (Bosnia-Herzegovina, FYROM, Georgia and Montenegro) cannot be treated as a homogenous group, but require individual approaches regarding their accession to NATO. FYROM already has the support of all NATO members except Greece, which is still blocking its admission. In December 2011, the International Court of Justice ruled 15:1 (the Greek judge being the sole dissenter) that Greece was wrong in blocking FYROM's accession to NATO at the Bucharest summit in 2008. It remains to be seen whether key allies like the United States will increase pressure on Athens to lift its blockade so that FYROM can join the Alliance, as it was initially scheduled to do in 2009.

With regard to Bosnia-Herzegovina and Montenegro, the application process is far advanced as the two countries are part of the MAP. Subject to sufficient steps being taken in terms of reform and preparation for membership, the ball will be in NATO's court to offer membership to both countries. Whether this could happen as early as the next NATO summit, which is likely to take place in 2014, will depend on consensus-building among the 28 Alliance members.

Georgia is a different case. After the membership guarantee given by NATO in Bucharest, the question is no longer whether Georgia will be admitted, but when. At the same time, Georgia is not yet part of the MAP, which is regarded (albeit with no formal statement to this effect) as a precondition for membership. The US in particular has been arguing that membership preparation could also be done within the NATO-Georgia Commission, omitting the time-consuming MAP process. Such a proposal, though, has precarious implications. The MAP not only prepares applicants for membership; by virtue of its unlimited time frame, it provides NATO with the necessary flexibility in decision-making on enlargement. Albania, for instance, joined the MAP in 1999 and maintained this status for ten years until it joined the Alliance in 2009. In other cases, the MAP phase was significantly shorter – according to the condition of the applicant state and the requirements of the overall political situation. Bypassing the MAP in the Georgian case would (again) create a precedent vis-à-vis other applicants, with potential negative implications in the long term. It would also deprive NATO of the possibility

to assess continuing development of the Georgia-Russia relationship and to bridge the different positions within the Alliance on Georgia's membership.

To move the enlargement issue significantly forward, but at the same time to take note of the special implications of a Georgian membership, the next summit should include Georgia in the MAP process. This would be a visible step ahead for Georgia, and it would be in line with NATO's previous procedures for admission. Moreover, such a step would provide NATO with breathing space for consensus-building.

NATO could also consider updating the 1995 *Enlargement Study*. Even if this document is still fundamental, a revision (including an appraisal of the membership policy NATO has pursued for almost two decades) might be useful.

An open door policy remains a core element of NATO's overall strategy for a *Europe whole and free*. However, enlargement does not need to follow what some in the European Union call the "*bicycle theory*", according to which it has to constantly move forward so as not to fall over. Instead, enlargement is an individual process which must certainly be pursued without external vetoes. At the same time, this does not imply that each and every membership application will progress to an automatic, foregone conclusion.



SECURING THE SAHEL: A ROLE FOR NATO?

Paul PRYCE

Against the background of the well established partnership programme that NATO has with several North African countries bordering the Sahel region of Africa, the author writes about some developments in the region that have been far less positive and which might soon demand greater attention from NATO member states.

Moreover, he mentions that it is in the role of “deep” conflict resolution that NATO could make an immensely valuable contribution, utilising mediation to prevent al-Qaeda from establishing a lasting foothold in the region while averting a protracted military conflict, at the same time expending minimal Alliance resources.

In the end, he considers that, at the same time, one of the most pressing moral challenges the Alliance will be confronted with in the coming year is whether NATO can render tangible assistance to one of the most impoverished and imperilled regions of the world. The awful events near In Aménas indicate what is now at stake.

Keywords: *Operation Unified Protector; Mali; Sahel; In Aménas; al-Qaeda; ECOWAS*

From start to end, 2012 saw the security situation in Libya and the Sahel develop rapidly. Some of these developments were decidedly positive, such as the peaceful transfer of power from the National Transitional Council to Libya’s elected National Congress in August. Yet there have been numerous other developments in the region that have been far less positive and which might soon demand greater attention from NATO member states.



While *Operation Unified Protector* was instrumental in removing the oppressive regime of Muammar Qaddafi from power, the lack

The article was featured in the *NATO Review*, the *What's 2013 Got in Store?* issue, 2012, <http://www.nato.int/docu/review/2012/Predictions-2013/NATO-Securing-Sahel/EN/index.htm>

Paul Pryce is a Lecturer of International Relations at the *Tallinn School of Economics and Business Administration*. He previously worked in conflict resolution as a Research Fellow with the OSCE Parliamentary Assembly.

The opinions in this article are those of the author alone and do not necessarily reflect those of the NATO Alliance or of any of its member states.

of a concerted international response on the ground in Libya left the country's considerable arms stockpiles largely unguarded. Thus, the aftermath of the Libyan civil war has seen the proliferation of sophisticated military equipment and experienced fighters across the region, bolstering Tuareg rebel movements and Islamic fundamentalist groups in areas of Mali, Burkina Faso, Niger, and elsewhere. The result has been growing instability across the Sahel region.

This fallout has been particularly detrimental in Mali. By May 2012, just a short few months after the conclusion of *Unified Protector*, a coalition of Tuareg rebels and Islamist groups loosely associated with al-Qaeda in the *Islamic Maghreb (AQIM)* proclaimed the independence of the "*Islamic Republic of Azawad*", encompassing vast swathes of territory in northern Mali. Fierce fighting soon followed, causing an estimated 65 000 Malians to seek refuge and relative safety in neighbouring Burkina Faso.



What lessons could be drawn from NATO's operation in Libya for the region?
© Reuters



How far can UN assistance in the region stretch?
© Reuters

Confronted with an emerging crisis in the Sahel, the international community has taken some steps to address the growing instability. In October, the United Nations Security Council adopted *Resolution 2071*, calling on the *African Union (AU)* and the *Economic Community of West African States (ECOWAS)* to develop an actionable plan for an intervention that would assist the lawful Malian government in exerting its sovereignty over all those territories internationally recognised as Malian. On 20 December, having received a rough outline from ECOWAS, the Security Council adopted *Resolution 2085*, authorising the AU and ECOWAS to move forward with their plan and calling for Tuareg rebel groups to sever ties with AQIM and its affiliates. As of January 2013, France has begun to provide military support to the Malian government, moving against insurgents in the northern regions of the country.

Resolution 2085 is only the beginning of a long effort that will require a steadfast commitment from all stakeholders to see a peaceful and prosperous

Sahel in 2013 and beyond. Central to these efforts must be the High Representative of the AU for Mali and the Sahel, as well as the yet to be appointed counterpart from ECOWAS. The work of these mediators holds the potential to address the deeper causes of conflict in the region, going beyond the simple deployment of military forces by the AU, ECOWAS, or France to counter the encroachment of AQIM. It is in this role of “*deep*” conflict resolution that NATO could make an immensely valuable contribution, utilising mediation to prevent al-Qaeda from establishing a lasting foothold in the region while averting a protracted military conflict, at the same time expending minimal Alliance resources.

In August 2012, Secretary General Anders Fogh Rasmussen appointed a new *NATO Special Representative for Women, Peace, and Security*. Both Jaap de Hoop Scheffer and Anders Fogh Rasmussen have appointed individuals to the office of *Special Representative for the Caucasus and Central Asia* during their respective tenures as NATO Secretary General. Much as these NATO Special Representatives can, and have, contributed meaningfully toward regional security cooperation, a NATO



NATO Secretary General, Anders Fogh Rasmussen, together with Mari Skåre, Secretary General's Special Representative for Women, Peace and Security.

© NATO

Special Representative for the Sahel could assist in mediation efforts in Mali, either spearheading discussions between the various factions or serving as backup to the mediators appointed by the AU and ECOWAS. As NATO member states express increasing concern over the potential for arms trafficking within the region, a NATO Special Representative for the Sahel could also prove to be an invaluable contact point between NATO, relevant African regional organisations, and Sahel countries themselves on counter-trafficking efforts.

In carrying out *Operation Unified Protector* in 2011, NATO has demonstrated both the willingness and the ability to intervene in conflicts taking place on the African continent. As such, the Alliance will soon be expected by many partners in the international community to weigh in on the situation in the Sahel. However, the military intervention pursued by ECOWAS and France risks exacerbating the conflict further, enkindling ethnic tensions while failing to build any confidence among northern communities in the central government of Mali. NATO would demonstrate a greater understanding of the conflict and improve



January's attack in Algeria highlighted some of the risks in the region
© Reuters

its capacity to address other emerging security issues in the region through the appointment of a Special Representative for the Sahel by the Secretary General.

Indeed, if NATO is to positively influence events in the Sahel, the Alliance must act quickly. The shocking and tragic attack by an al-Qaeda affiliated group on an Algerian gas facility near In Aménas demonstrates the potential for regional conflicts to deepen and spread beyond Mali's territory. As of this writing, the death toll is estimated to be at least 80. Mokhtar Belmokhtar, the leader of the group responsible, has promised further such attacks. A disjointed response,

consisting of unilateral actions by individual states, will only see the situation continue to deteriorate. A concerted response by an international actor like NATO, possessing the diplomatic weight of 28 countries and the expertise of a Special Representative, could avert further violence and bloodshed.

Entering 2013, one of the most pressing questions facing NATO is whether the Alliance can coordinate effectively with other security actors to secure shared interests. At the same time, one of the most pressing moral challenges the Alliance will be confronted with in the coming year is whether NATO can render tangible assistance to one of the most impoverished and imperilled regions of the world. The awful events near In Aménas indicate what is now at stake.



NATO'S DEALING WITH A DIFFERENT GULF NOW

Jean-Loup SAMAAN

The article is intended to review the eight years that followed the initiation of the Istanbul Cooperation Initiative between NATO and selected countries in the broader region of the Middle East.

In this context, the author looks at whether the Alliance needs to change its approach to Arab countries post-Arab Spring, how these changes could look and how to overcome obstacles, given that the implementation of an ambitious but at the same time realistic strategic dialogue with Gulf countries could help the Alliance reassess its approach to the Middle East.

To conclude, he writes that, in order to prevent the ICI becoming irrelevant in the future, one must refine its methodology and agenda priorities – to bring it closer to NATO and ICI partners' security concerns.

Keywords: ICI; GCC; partnership; smart defence; Operation Unified Protector

Eight years after NATO initiated its engagement with Gulf countries through the *Istanbul Cooperation Initiative (ICI)*, the results have been modest, not to say disappointing.

This is paradoxical, even troubling, when one considers the genuine strategic relevance of the ICI. Indeed the Gulf is – and for the near future is likely to remain – a critical region for NATO. It encapsulates all the major security challenges the Alliance aims to tackle: maritime security, risks of proliferation of nuclear weapons, as well as state failure.



The Istanbul Initiative was signed in very different times
© Reuters

The article was featured in the *NATO Review*, *The Arab Spring – What Now?* issue, 2012, <http://www.nato.int/docu/review/2012/Arab-Spring/NATO-Gulf-Strategic-Dialogue/EN/index.htm>

Jean-Loup Samaan is a researcher at the NATO Defence College in Rome, Italy. The views expressed here are his alone.

Moreover, in times of financial austerity in NATO countries, the partnership approach increasingly appears the most appropriate way to share the burden between allied members and local partners, thus creating a pragmatic division of labour.

Learning the lessons of the ICI

Back in 2004, the initial assumption behind the ICI was that the political realm of the partnership would not suffer the same obstacles that NATO's *Mediterranean Dialogue (MD) programme* had encountered. The MD was supposed to use the Oslo peace process between Israel and the Palestinian Authority to reinforce political and security cooperation between NATO and its neighbours on the southern shores of the Mediterranean. But following the breakdown of the diplomatic talks, implementation of the MD became extremely difficult.

At first sight, the political environment of the ICI looked much more favourable to cooperation. There was no issue among the partners as contentious as the Israeli-Arab issue. The ICI was therefore designed using a reversed pattern. While MD would focus on overcoming political obstacles through diplomatic dialogue, the ICI would adopt a bottom-up approach by building practical military-to-military ties to flesh out the political rapprochement.

However, from the start, NATO encountered several obstacles:

First, Saudi Arabia and Oman, which account for approximately 70% of the Gulf countries' defence expenditures, did not join the ICI. True, Oman did not completely reject cooperation with NATO. And over recent years, there have been numerous indications that the Sultanate favoured closer relations.

However, caution and balance tend to prevail in Muscat's posture towards NATO. The popular narrative in the Middle East

portrays the ICI as a NATO-GCC alliance against Iran. This would be embarrassment for Oman, which aims to maintain good political relations with Tehran.

In the case of Riyadh, such a narrative is less unsettling. But Saudi Arabia, being the regional powerhouse, did not want to be put on a par with small Gulf kingdoms that rely heavily on external powers for their security. If Saudi Arabia was to establish formal relations with NATO, it would have to be a tailored,



Countries part of the Gulf Cooperation Council

one-on-one framework. Overall, Saudi Arabia's leadership of the GCC underlines the difficulty NATO will have playing a role in the region without engaging Riyadh.

The second obstacle to ICI's advance is its failure to "*multilateralise*" its process. The Gulf countries that joined the ICI (Kuwait, United Arab Emirates-UAE, Qatar, and Bahrain) expressed their preference for a bilateral framework, rather than a multilateral one. They wanted to engage with NATO. But on their own. Not side by side.



The dialogue continues
© NATO

The ICI partners have approached NATO's initiative the same way they approached their multiple national security arrangements and guarantees with western powers. Because of wide geopolitical divergences and some mistrust between GCC countries, they have sought close bilateral relations to pursue their own distinctive diplomatic goals.

The prevalence of bilateral defence agreements among Gulf countries has led to few collective priorities, inconsistent military-to-military relations, and unnecessary capabilities redundancies. Consequently, officials from Gulf countries tend to ignore their neighbours' agenda with NATO, and formulate their own strategies without envisaging a precise regional dimension.

But this is only one part of the equation, and one that NATO obviously cannot control. Regarding the partnership *per se*, the Alliance should waste no time in reconsidering its bottom-up approach.

The case for a NATO-Gulf strategic dialogue

Some achievements in NATO-GCC relations are worth considering and using. For instance, the Gulf countries have been amongst the most active partners in NATO-led operations (the UAE and Bahrain in ISAF; the UAE and Qatar in *Operation Unified Protector*). These achievements prove that what is at stake

is not NATO's Gulf policy as a whole but the ICI as a means of implementing it. I have heard this paradox emphasised by some Brussels insiders who argued that these successes could well have taken place anyway.



How to adapt to the new reality?
© NATO

To prevent the ICI becoming irrelevant in the future, we must refine its methodology and agenda priorities – to bring it closer to NATO and ICI partners' security concerns.

The first imperative is to extend the bilateral nature of the ICI: the multilateral track should become its core arrangement. This could be developed by creating a strategic dialogue between ICI partners held twice a year, once in Brussels and then once in one of the Gulf capitals. Additionally, Saudi Arabia and Oman could be able to attend as special observers.

The dialogue could include a political dimension by gathering together ministers and chiefs of defence. But its effectiveness would depend on a calibrated mix of diplomats, desk officers and scholars from both sides discussing the ICI agenda. In other words, this NATO-Gulf strategic dialogue should not be a classic, very formal and official gathering but a platform to exchange fresh ideas and promote future cooperation.

A NATO-Gulf strategic dialogue could redirect the partnership towards its long-term goal and include the discussion of timely policy issues such as maritime security, capability-building and countering security vacuums. It could also be used to discuss the stand-off with Iran.

The Iranian issue should not be treated casually. The Iran-threat perception in the Gulf has to be considered with caution. But here too NATO could play a key role in preventing unintentional escalation. Eventually, NATO and GCC countries



Bahraini forces in Afghanistan

will have to find a more or less formal framework to shape some kind of deterrence dialogue with Iran. This subset of the NATO-Gulf strategic dialogue would logically engage NATO partners, as well as the Iranians. It would not necessarily involve high level national representatives and would very likely remain at the second-track level.

Though it might sound far-fetched, there is nothing in theory that prohibits Iran from participating in ICI discussions. Still, several political issues would have to be cleared up before: the nature of Iran's nuclear programme, the willingness of both NATO members and partners to engage with Iran and the compatibility of such an initiative with the current UN, US and EU sanctions regime targeting Tehran. But in the long run, a dialogue



*The UAE already has some impressive hardware
Courtesy Lockheed Martin*

of this kind could provide a framework in which to discuss respective military postures, exchange assessments on potential flashpoints, design safety valves and eventually to avoid miscalculation.

In general terms, an agenda for NATO-Gulf strategic dialogue may have to accommodate the national preferences and inclinations of the 28 allies, in particular those who already have special relations with the GCC as a whole or/and with its individual countries. But owing to the interdependence between stakeholders in the security issues mentioned and also to the allies' new emphasis on cooperative security, this dialogue would not be redundant.

So – what to do?

Lessons from its eight years of existence show that the issue at stake is not the purpose of the partnership itself but rather its methodology.



Qatar puts its weight behind the NATO Operation Unified Protector for Libya

In that perspective, it relates to a broader challenge for NATO. Namely that, as the organisation struggles internally with the financial crisis, it is revising its global posture through the concept of “*smart defence*” which aims to extract greater value from reduced defence budgets through closer cooperation. As suggested above, cooperation with ICI partners during *Operation Unified Protector* may well be one of the closest illustration of “*smart defence*” practices we can achieve.

This is why the implementation of an ambitious but at the same time realistic strategic dialogue with Gulf countries could help the Alliance reassess its approach to the Middle East.

More than a century ago, when his laboratory faced bankruptcy, the physicist Lord Rutherford said to his colleagues: “*Gentlemen, we are out of money. We’ll have to think*”. As the transatlantic allies face similar difficulties, they should indeed start thinking about smart partnerships.



Seminar

Capability Identification, Planning and Development in the Romanian Armed Forces

Captain (N) Theodor Nicolae ENACHE

Between 26 and 27 March 2013, under the auspices of the Deputy Chief of the General Staff, Lieutenant General Dr Dan GHICA-RADU, it was held in Bucharest the Seminar on *Capability Identification, Planning and Development in the Romanian Armed Forces*, organised by the General Staff and the Department for Defence Policy and Planning, with the participation of the Capability Development Directorate within the Staff Element Europe – SEE in Mons, Belgium, a structure belonging to the Allied Command Transformation – ACT, Norfolk, USA, and NATO Communications and Information Agency – NCIA.

The activity was planned by the Strategic Planning Directorate – SPD, being a continuation of the visits of ACT delegations in March – ACT Nations Engagement Team – NET, September – capability development support team,



Captain (N) Theodor Nicolae Enache – the Strategic Planning Directorate, the General Staff, the Ministry of National Defence.

and in November 2012 – the team to review the capabilities available to NATO through NATO Defence Planning Process – NDPP. This activity is part of the ACT programme to support NATO member states in developing capabilities. The activity was attended, besides the Deputy Chief of the General Staff, Lieutenant General Dr Dan GHICA-RADU, by chiefs and deputy chiefs of directorates within the General Staff, deputy chiefs of the Armed Forces Services, representatives of the Department for Defence Policy and Planning, unit commanders, “Carol I” National Defence University teaching staff members and students.

To facilitate the participation of more people interested and involved in the process of defence capabilities development and defence planning, the event unfolded over two days, the first at “Carol I” National Defence University, to allow the participation of the students in this institution, and the second at the Ministry of National Defence “Haiducului” transit-accommodation and representation centre, when participated experts, personnel within the General Staff structures as well as within subordinate structures having responsibilities in the field. Thus, over 120 people attended the event during two-day meetings.

On the first day, ACT team made several presentations related to NATO’s defence planning process. The participants were informed about the importance attached to defence planning within NATO, the structure of the process and the key participants in this process. In addition, the main steps of NATO defence planning process were reviewed and NATO structures having responsibilities for this process were described.

The discussion sessions as well as the question-and-answer sessions, held after each presentation made by ACT representatives, were complex and highly interactive. The participants in the seminar requested clarifications on the processes and procedures related to defence planning, on the way a parallel



between national and NATO processes can be drawn, and on the implications of this aspect. Moreover, information was asked regarding the advantages of capability-based defence planning compared with other types of defence planning such as threat- or budget-based defence planning. The participants were also interested in the connection between the Planning, Programming, and Budgeting System – PPBS and defence planning as well as in the government structures responsibilities within a capability-based defence planning national process. ACT team members answered all the audience questions in a professional manner.

The second day was dedicated to specialists in the field. Representatives of the structures within the General Staff and of the subordinate structures as well as of the Department for Defence Policy and Planning having responsibilities for capability development and defence planning attended the seminar. There were presentations on defence planning requirements and target capabilities implementation. SPD representatives made a presentation regarding Romania's participation in the two multinational capability development initiatives, NATO *Smart Defence* and the European Union *Pooling & Sharing*. As on the first day, after each presentation, question-and-answer sessions were held. As expected, the discussions were interactive, highly professional and technical. The main topic of debate was the way to ensure and implement the capabilities that the Alliance needs as well as the interconnection of the national process of identifying capability needs and developing the necessary capabilities with the Alliance capability needs. One of the issues raised was the necessity to align national defence planning processes with that of NATO. In this context, it was highlighted that the alignment would facilitate the planning process as such, as well as the coordination and communication between national decision makers and NATO experts.

In conclusion, based on the discussions during the seminar, the ACT team presentations, and the participants' interventions, the following key aspects can be highlighted: capability-based planning is proved to be the appropriate defence planning process in the current global context; the alignment of national defence planning process with NATO one represents the main element in ensuring the key capabilities that may be placed at the Alliance's disposal; the development of defence planning software (e.g. IG TOOL), classified at the necessary level, having access to a database containing all the capabilities that may be placed at the Alliance's disposal, will make defence planning more effective; at national level, a way to set in motion the mechanism concept development, experimentation, capability development and implementation should be found; a strong conceptual basis is necessary for effective capability development programmes.

English version by
 **Diana Cristiana LUPU**

CONFIDENCE AND SECURITY BUILDING IN THE WIDER BLACK SEA REGION THROUGH MULTINATIONAL COOPERATION WITHIN SMART DEFENCE AND POOLING & SHARING INITIATIVES

Captain (N) Vicențiu CĂTĂNEANU

The concept of NATO's Smart Defence initiative is aimed at using with maximum efficiency (smartly) the resources for defence, with the purpose of maintaining the Alliance capacity of carrying out its missions and is based on multinational cooperation.

It was the main topic on the agenda of the NATO Chicago Summit on 20-21 May 2012.

The goal of the EU Pooling and Sharing initiative is to identify and implement new projects for achieving EU defence capabilities by using development and shared use of capabilities mechanisms in the multinational framework.

The P&S concept was highlighted in 2008, following a study of the European Parliament, being then assumed and promoted by EDA, starting with 2009.

Keywords: *Smart Defence; Pooling and Sharing; NATO; the EU; multinational cooperation; Wider Black Sea Region; ACT; EDA*

Multinational cooperation within the two complementary initiatives, for the development and shared use of military capabilities, can provide significant economic and financial advantages, depending on the resources and association interests of participating states, and can bring about increasing mutual confidence, as an element of the economic stability and prosperity that is extremely necessary given the general austerity generated by the long-lasting global financial crisis.

Launching joint regional projects meant to narrow the capabilities gap can be beneficial, and lowering the military facilities exploiting and operating costs, initially in fields such as education, training or logistic provision, can lie at the basis of the consequent development of broad projects that can be supported by EU and/or NATO structures. In this context, Romania analyses the regional cooperation opportunities seeking to achieve and jointly exploit capabilities relevant for national defence from the position of important

Captain (N) Vicențiu Cătăneanu – Deputy Chief, the Strategic Planning Directorate, the General Staff, the Ministry of National Defence.

stability generating factor in the region and important NATO and EU border state, riparian state of the Wider Black Sea Region, which is an area of extraordinary geostrategic interest, due first of all to the energy corridor that feeds Europe.

In the context of the need for security felt by many unaligned states in the Wider Black Sea Region, the fact that the two initiatives are open to the participation of non-NATO or EU makes the possible involvement of many actors in the mentioned area more attractive. It is obvious that, because of the level of classification of the details regarding participation, only the projects from certain fields (for instance: common training/firing exercises, crisis management, natural and man-made disaster relief, equipment maintenance, possibly air policing, military education etc.) will be open to the participation of these states.

Reviewing the history of the involvement of non-NATO and EU states from the Wider Black Sea Region in NATO and EU initiatives, projects and missions, for instance ISAF (*Operation Enduring Freedom – OEF with NATO Training Mission – Afghanistan – NTM-A*), *Operation Iraqi Freedom – OIF with NATO Training Mission – Iraq NTM-I*, *Blackseafor*, *Black Sea Harmony*, *Atalanta*, *Ocean Shield* or within regional initiatives such as *South Eastern European Brigade – SEEBRIG*, we can be optimistic and not rule out the participation of most Black Sea riparian states to *Smart Defence – SD* and *Pooling and Sharing – P&S*, considering the possible financial advantages related to these initiatives.

NATO's Smart Defence Initiative

The concept of *Smart Defence* is aimed at using with maximum efficiency (smartly) the resources for defence, with the purpose of maintaining the Alliance capacity of carrying out its missions and is based on multinational cooperation on three specific courses of action:

- *to identify and set up a hierarchy of critical capabilities requirements* – the *Lisbon Critical Capabilities Package – LCCP* was agreed upon, the defence planning process was reviewed with the purpose of guiding it towards covering deficient areas and special attention is paid to using the lessons learned from current operation in developing future capabilities, as well as to setting up a system of indicators that should provide the Alliance with the capacity of timely assessing the results for efficiently guiding the efforts towards priority capabilities;
- *to promote a broad cooperation in the field of defence* – the need for close cooperation between the allies as far as defence programmes are concerned, the maximum use of NATO-EU cooperation relations and the concerted efforts of relevant NATO committees were pointed out;

- *to develop NATO capabilities through innovative multinational approaches* – the concept stipulates that NATO should assume an active role, of catalyst of the relations between member states, for identifying and exploiting the opportunities that can contribute to achieving capabilities in the multinational framework.

The multinational solution is not a recent idea and entails a series of elements that should strengthen the chances for such an approach to be successful: *1. pragmatic approach based on mutual political and economic interests and the own definition of defence; 2. initiation of a dialogue between ministers of finance and armament directors; 3. provision of resources according to the 2% of the GDP engagement, by imposing sanctions for a smaller percent; 4. cooperation for the development of a major defence capability able to also cover the design and development stages, and not just the final one, of acquisition; 5. a real cooperation with the European Defence Agency – EDA.*

In March 2011, during the informal meeting of the ministries of defence of NATO member states, the Alliance Secretary General promoted the *SD* concept and underlined that the defence budget cuts of European states brought about an imbalance on three dimensions: *1. capabilities gap between the USA and the European states; 2. increasing capabilities deficit at European level; 3. increased dependency upon American capabilities.*

Within the *Allied Command Transformation – ACT*, the *Task Force on Building Capability through Multinational Approaches – ACT TF* was established, organised in five working groups with members from *ACT*, *Allied Command Operations – ACO*, known especially as *Supreme Headquarters Allied Power Europe – SHAPE*, *International Military Staff – IMS*, *International Staff – IS*, *NATO Headquarters – NATO HQ*, *NATO Support Agency – NSA* and in connection with national and EU representatives.

Each working group was in charge of a specific domain, as follows: *capabilities and force structures* for an efficient NATO-EU cooperation and harmonisation with the efforts of development and shared use of capabilities at EU level (*Pooling & Sharing*); *defence acquisitions* for searching and identifying multinational approach opportunities that enable a fair share of the high costs related to purchasing and operating modern systems; *operation and maintenance* for the identification of multinational cooperation opportunities, either through *NAMSA* or in direct relation with industrial partners; *preparation and organisation of armed forces* for exploiting existent types of forces and multinational commands and promoting most efficient solutions; *innovative solutions* for exploiting and implementing the most modern

means in the field of capabilities development in the relation with the defence and research industry.

SD was the main topic on the agenda of the *NATO Chicago Summit* on 20-21 May 2012. One of the goals of the summit was the launch of a sufficiently credible and ambitious projects package (*Defence Package*), which should strengthen this initiative regarding the following domains: 1. *military intelligence, surveillance and research*; 2. *anti-missile (ballistic) defence*; 3. *force protection*; 4. *common force training*; 5. *support*.

Currently, at NATO level, there are 150 projects on three tiers. In *Tier 1*, there are included the projects that have a leader nation. In *Tier 2*, there are the projects of interest for the NATO member states that could be promoted to *Tier 1*. *Tier 3* mainly consists of projects proposed by state or organisations in NATO that try to involve the interested states and, implicitly, to get to *Tier 2*.

Romania is part of 40 out of 150¹ initiatives, as follows:

- *Tier 1*: 14 initiatives out of 25;
- *Tier 2*: 19 initiatives out of 58;
- *Tier 3*: 7 initiatives out of 67.

Currently, the structures belonging to the Ministry of National Defence that have responsibilities in this field analyse the opportunity of our country becoming involved in other 4 projects regarding the development and shared use of capabilities, one of them being proposed in *Tier 1*.

European Union's Pooling and Sharing Initiative

The goal of the EU *Pooling and Sharing* initiative is to identify and implement new projects for achieving EU defence capabilities by using development and shared use of capabilities mechanisms in the multinational framework.

The *P&S* concept was highlighted in 2008, following a study of the European Parliament, being then assumed and promoted by *EDA*, starting with 2009. *P&S* is intended as a resource management method that gathers the similar capabilities that are to be used through a central authority (*pooling*) or which gathers different resources for the achievement of a capability that will be used in common (*sharing*). As we have already mentioned, the issue is addressed by NATO as well through the similar *Smart Defence* initiative through *Multinational and Innovative Approach – MNIA*.

¹ According to *Status Report NATO DI (STR) (2012)0008 Update 18 REV17*, on 05.03.2013.

During the discussions from the informal reunion in Ghent (2010), Germany and Sweden presented a common reflection document that affirmed the need for identifying certain new domains of multinational cooperation for the accomplishment of EU goals undertaken through the *Common Security and Defence Policy – CSDP* and assumed the following stages for the implementation of the *P&S* initiative:

- a systematic analysis conducted by EU member states regarding the national military capabilities in order to identify multinational cooperation propositions for *P&S*;
- centralisation of results of national analysis by *European Union Military Staff – EUMS* and *EDA* and presentation of an integrated document to the ministers of defence for decision-making;
- identification by the member states of the projects and partners suitable for cooperation;
- facilitation and coordination of various initiatives by EU structures in the field.

In keeping with the conclusions of the *Political and Security Committee (PSC)* of the EU for implementing the conclusions of the Council on 9 December 2010, the *European Union Military Committee – EUMC*, in close cooperation with the *Crisis Management and Planning Department – CMPD* and *EDA*, centralised the results of the analyses conducted by member states, regarding the new possibilities of cooperation at European level for capabilities development.

At the same time, at *EDA* level, the *EDA Steering Board* decided to identify all opportunities regarding *P&S*, to set up a calendar and to develop opportunity studies. In March 2010, the calendar of the activities was agreed upon, with the following stages:

- *Stage 1* (2010) – inventorying existent initiatives and new opportunities in the field;
- *Stage 2* (2011) – identifying optimal solutions to case studies, assessing and selecting opportunities, defining priority and selection criteria;
- *Stage 3* (2012) – prioritising opportunities, setting individual calendars regarding specific capabilities and developing business cases.

At *EUMC* level, all member states sent propositions and the results of the *EUMS* confirmed the already identified tendencies for the regionalisation of cooperation, including the initiation of projects by a reduced number of states, a determining factor in the proposition of new European projects being *their impact on national sovereignty*. Thus, many propositions were made for education and training, considered as a domain with reduced impact on sovereignty, but certain projects specific to carrying out military actions were also proposed (air policing,

maritime patrolling), which proves a significant increase in the general confidence and transparency at the level of EU member states.

During *EUMC/Chiefs of Defence – CHODs* and the *Foreign Affairs Council* reunions, at the level of ministers of defence, it was acknowledged the importance of the document containing the results of the analyses conducted at the level of member states, for the multitude of solutions proposed, given the circumstances of the difficult financial environment and the participants agreed upon sending the end results of the analyses to the *Chairman of the EUMC – CEUMC*, by the end of September 2011. Following the analysis of the responses sent by the member states to the second request of the *CEUMC* (17 June 2011), the following relevant aspects resulted: the member states were mainly concerned with reducing the impact of defence budget cuts, especially on the possibility of ensuring the participation in *CSDP* operations and less with covering certain already identified capabilities gaps; the 171 clearly set initiatives were identified, including already initiated NATO and *EDA* ones, and, in the end, 116 propositions were considered useful; among them, 15 projects were evaluated as being potentially achievable. Following bilateral discussions with member states, the group of voluntary experts presented informally to the *EDA* Executive Director the following propositions: *the need for defining a new concept of sovereignty integrated at EU level; the phased approach to the initiative; the need for defining the financing mechanism; the identification of the ways to maintain the necessary capabilities for CSDP; the need for inter-ministerial analysis.*

Romania identified a limited number of areas of interests, out of the *EUMC* list, correlated with the *EDA* list. The national propositions that were communicated to the *EUMC*, after the approval of the Minister of National Defence, are aimed at participating in the following seven areas of interest: *medical support for operations, Counter Improvised Explosive Devices C-IED, CBRN capabilities, strategic airlift fleet, logistic support, aircraft pilots training and shooting ranges.* Currently, Romania is participating in certain important projects developed within *EDA* and which are part of the initiative, such as: *Theater Exploratory Laboratory – Demonstrator TEL-D, European Air Transport Fleet – EATF* and *European Satellite Communications Procurement Cell – ESCPC.*

Possible Developments in the Wider Black Sea Region Riparian States in Regard to the Two Initiatives

At NATO and EU level, it is required that the working framework/methodology for applying such an extremely complex process is clarified in order to allow the participation of non-member states (purpose, objectives, applicability fields, responsible structures, time-related aspects), as well as that this possibly new process

is correlated with other already ongoing ones: the EU – *Capabilities Development Plan – CDP* and *Headline Goal – HLG* and the national ones. At the same time, one will have to support cooperation with national factors with responsibilities in the field, and with NATO and the EU, with a view to avoiding duplication of efforts and providing complementarity in actions and mutual support between the two organisations, member and non-member states.

It is necessary for the Euro-Atlantic structures to be involved in carrying out the process, especially because of their role in: raising the subject at political level; enabling the exchange of information at the required level depending on the agreements signed in the field, between NATO, EU bodies and member states with non-member states participating in projects within the two initiatives; providing viable tools for enabling cooperation between member and non-member states; promoting possible solutions for future projects (including through standardisation).

English version by
✍️ *Iulia NĂSTASIE*



FRENCH GEOPOLITICS IN THE FAR EAST IN THE SECOND HALF OF THE 19th CENTURY

*Captain (N) Dr Olimpiu Manuel GLODARENCO
Captain (N) Ionel Dan CIOCOIU*

The French interest in northern Vietnam dated from the late 18th century, when the political Catholic priest Pigneau de Behaine recruited French volunteers to fight for Nguyễn Ánh to start the Nguyễn Dynasty in an attempt to gain privileges for France and the Roman Catholic Church. In 1858, France began its colonial campaign and in 1862 annexed several southern provinces of Vietnam to become the colony of Cochinchina, laying the foundations for its later colonial empire in Indochina. French explorers followed the course of the Red River through northern Vietnam to its source in Yunnan, arousing hopes that an extremely profitable overland trade route could be established with China, bypassing the treaty ports of the Chinese coastal provinces. The main obstacle to the realisation of this dream was the Black Flag Army, a well-organised bandit force under a formidable leader, Liu Yongfu (Liu Yung-fu), which was levying exorbitant dues on trade on the Red River between Sơn Tây and the town of Lào Cai on the Yunnan border.

Keywords: *Cochinchina; Tonkin; Annamites; Admiral Amedee Courbet; BAYARD; Siam*

Military Operations in Annam and Tonkin (1882-1884)

The indifference displayed by France to the colonial problems between 1871 and 1880 encouraged the Court at Hue not to fulfil their obligations stipulated in the *Treaty of Saigon* in 1874, on the protection of the freedom of trade in Tonkin. Thus, French merchants were subject to continuous insults of the mandarins or suffering due to the *Black Flag* (local combat groups).

Not only that the Vietnamese Government did not do anything to recall officials at their debts or to repress acts of robbery of the Black Flag, but continued to maintain old relationships with China, bondage which encouraged the latter to assert itself in the fight against French influence in Tonkin. China, which did not recognise the Treaty of 1874, was looking skilfully for every opportunity that was offered to oppose the French actions.

Captain (N) Associate Professor Dr Olimpiu Manuel Glodarencu
– Director, the Romanian Navy Museum, Constanța.
Captain (N) Ionel Dan Ciocoiu – Statul Major al Forțelor Navale.

Regular Chinese troops were introduced, little by little, in Tonkin, under the benevolent eyes of the Annamites authorities (name given to the Vietnamese until 1945).

Things got worse, more and more, until 1881, when colonial ambitions awoke in France. At this point, the situation that was developing in Tonkin retained the attention of the French Government, which decided to intervene.

On 25 March 1882, Captain Henry Laurent Rivière (1827-1883), Commander of the Cochinchina Navy, was sent to Tonkin with three gunboats and a detachment of 700 men to restore order and to impose respect for the interests of France. The instructions recommended pacifist actions, but he acted contrary by occupying the military citadel of Hanoi (25 April 1882).

In Paris, the emotion was great when finding out this news. The Minister of the Navy immediately ordered General Alexandre-Eugene Bouet (1833-1887), Commander of the troops in Cochinchina, to move to Tonkin, where troops were to be seriously strengthened, and, under the orders of Rear Admiral Anatole-Amedee-Prosper Courbet (1827-1885), established a squadron for Tonkin, different of that of China Sea, commanded by Rear Admiral Charles Meyer, which was also strengthened. In the meantime, by the Decree of 8 June 1883, Francois Jules Harmand (1845-1921) was appointed civilian Commissioner General of Tonkin.

Admiral Courbet arrived in the Gulf of Along with the battleship *BAYARD*, in the second half of July. On 30 July, a meeting took place between Courbet, Harmand and Bouet at Haiphong to analyse the situation and to propose a solution to the Government. The conclusion was that a direct and energetic pressure on the Annamite Government was necessary through naval demonstrations in front of Thuan-An, simultaneously with the occupation of the forts at the entrance to the Hue River.

The French Government approved the project and Admiral Courbet arrived in front of Thuan-An on 18 August 1883, onboard battleship *BAYARD*, accompanied by ironclad *ATALANTE*, cruiser *CHÂTEAURENAULT*, gunboats *LYNX* and *VIPÈRE*, aviso *ALOUETTE* and 2 transporters, *ANNAMITE* and *DRAC*, which had onboard 600 marines, a company of Annamites riflemen and a battery of artillery. The Admiral prompted the Annamites authorities to surrender the forts in two hours, under the threat of bombardment. When time expired, the entrance was bombed, from 16.30 to 20.00. The Annamites forts unsuccessfully fired back, with an intensity that fell rapidly.

The landing, hampered by stormy weather, was unable to be executed until the morning of 20 August, under the protection of naval artillery, highlighting gunboats *LYNX* and *VIPÈRE*, which went close to the shore as much as possible. The landing companies of two battleships and the cruiser, following the troops

that already set foot on shore, neutralised the resistance of Annamite soldiers. At 09.00 that morning, French flags replaced the Annamite flags on top of main forts. Gunboats *LYNX* and *VIPÈRE*, advancing together, passed through to the artillery barrage made by the last Annamite guns at the mouth of the river, getting ready to steam up river, to the capital.

The success of the operation was complete. During the night, the Annamite Government called for a ceasefire, which was granted. During that time, Jules Harmand sent an ultimatum that contained the French conditions.

The conditions were accepted. The Treaty of Hue, signed on 25 August 1883, recognised the French protectorate over Annam and Tonkin. France would set the directions of foreign policy, including China. Among other provisions, France took the responsibility to hunt the *Black Flag* from Tonkin and to ensure communication and trade freedom.

After the operations at Thuan-An, the ships of Tonkin squadron maintained the coastal blockade for ten months, to prevent weapons smuggling, or to patrol at the mouth of the River Hue in the flank of the French Garrison stationed in the forts. Only the gunboats continued to carry out active war missions in cooperation with the Expeditionary Corps.

But, the operations evolved very slowly, because the troops were insufficient. Moreover, they suffered from disagreements between the Commissioner General and General Bouet. Because disagreements worsened, the French Government decided, in October 1883, to recall the General and to appoint Admiral Courbet as commander of naval and land operations of Tonkin. In these circumstances, Admiral Courbet moved his staff from onboard of his flagship and set up a headquarters in Hanoi, on 26 October, including a battalion of 600 marines. As soon as reinforcements arrived from France, he made up an expeditionary corps of 9 000 soldiers and sparked a strong offensive, from 14 to 17 December. The result was the capture of Son Tay Fort, the enemy's retreat started to north and the Delta was released.

The colonial army generals were touched in their pride, because their troops were commanded by a sailor. When, due to the successive supplements, the army of occupation reached 15 000 people, the command was given to a General.

Admiral Courbet was replaced on 12 February 1884, by General Charles-Théodore Millot (1829-1889), right when he was preparing to use the same manoeuvre to take over Bac-Ninh as at Son-Tay. Although, on 1 March, he received the rank of Vice Admiral for the brilliant work performed, he was unhappy to return aboard ship *BAYARD*, where he could not demonstrate his abilities, in a useful manner. Fate booked a lead role for him not in the waters of Annam and Tonkin, but in China's seas.

Naval Retaliation against China (1884-1885)

The modification of Admiral Courbet's missions occurred because of a serious event in Tonkin, in June 1884. According to the preliminary Convention signed at Tientsin on 11 May 1884, whereby China would withdraw its troops from Tonkin on 6 June, a column of 600 French soldiers, commanded by Lieutenant Colonel Dugenne, was sent to Langson to occupy that city. The French unit, arriving around Bac Le on 23 June, met a corps of 10 000 regular Chinese troops. As a result of the fight, the French unit was forced to retreat towards Phulang Thuong after suffering heavy casualties.

After the ambush, the French Government ordered Admiral Courbet to leave Tonkin with his squadron, to take command of all naval forces deployed in China's seas and to enforce the terms of convention.

The Admiral left the bay of Along on 29 June and moved to Shanghai, where he met Jules Patenotre de Noyers (1845-1925), French Minister to China, together with whom he established the terms of an ultimatum addressed to the Chinese Government and the following necessary military operations.

In his opinion, the Chinese fleet and arsenals on Foutcheou and Port-Arthur had to be hit first, proposing an immediate naval action against the Foutcheou Naval Base and upon the ships out there. He also considered a similar action against the arsenal in Port-Arthur and Wei-Hai-Wei Naval Station, action to be carried out with the help of Admiral Sébastien Lespès's (1828-1897) squadron, stationed at that time in the Gulf of Petchili. Finally, he suggested sending warships to Nankin for an ambush.

Nevertheless, the French Government decided not to rush the action, hoping to defeat the Chinese resistance through intimidation, without violence. It was reluctant in disturbing the foreign nations interests in China.

In these circumstances, Admiral Courbet's proposals were not approved and he was authorised to return to Foutcheou and to post his ships in front of Keelung Harbour, located north of the Island of Formosa. The formal order was to refrain from any kind of hostilities until further order.

Complying with these provisions, the Admiral sent the cruiser *VILLARS* in front of the Keelung Harbor, and then moved his flag on light cruiser *VOLTA* and anchored on 16 July, at Foutcheou. *DUGUAY-TROUIN*, *ASPIC*, *VIPÈRE*, *LYNX*, *CHÂTEAURENAULT* and two small torpedo boats, hull number 45 and 46, followed him successively. Admiral Lespès's squadron was recalled in the waters of Petchili.

In the mean time, the initiative remained with the diplomats. A first ultimatum, which was supposed to expire on 19 July, was sent on 12 July to the Chinese Government.

On 18 July, the expiry date of the ultimatum was extended until 1 August. A final period of 48 hours was granted on 31 July. Exasperated to wait for a favourable response that would not arrive, the French Government resumed its freedom of action on 2 August.

Admiral Courbet was ordered to send Admiral Lespès to Formosa to destroy the fortifications of Keelung and conquer the coal depot. Lespès, onboard of *VILLARS*, met in front of the port of Keelung, on 4 August, the battleship *GALISSONNIÈRE* and the gunboat *LUTIN*. Immediately, the Chinese General was summoned to surrender the defensive system. Because the request remained unanswered, in the morning of 5 August, the French ships began shelling. The Chinese responded quickly and with precision, but the fight back was short-lived. After nearly an hour, all the fortifications were rummaged and abandoned by defenders. The French landing companies destroyed Chinese war material and installed the camp there. Next morning, while trying to advance and occupy the small town of Keelung, the French troops were impacted by a Chinese unit consisting of several thousand soldiers. Overwhelmed by the large number of the enemy, and in danger of being encircled, the French troops withdrew, not without serious losses.

This demonstrated that, without the contribution of a strong detachment of landing troops, it was impossible to occupy Keelung and the coal deposits located at 6 kilometres from the harbour, behind some steep hills.

Admiral Courbet continued actions in front of the Foutcheou Harbor. After twenty days of waiting, eager for action, he urgently asked for the authorisation to trigger hostilities, signalling that the inactivity of French forces would have ruined their morale and that the time lost would have favoured the Chinese, who undoubtedly strengthened the defensive means. The Government responded that he should wait, although the failure of Keelung fuelled Chinese pride and offered them a reason to resist the French claims. The French Government continued, however, to promote a satisfactory diplomatic solution. Weeks passed, and the situation of the Courbet squadron in front of entrance of Min River became increasingly difficult. The time spent in inactivity by the French was extensively used by the Chinese forces to become increasingly stronger and better protected. The French ships were on alert, but the anchorage area at Foutcheou was transforming, more and more, in a kind of trap. This situation lasted until 22 August, when the Government finally gave Admiral Courbet the order to attack the Chinese fleet and destroy the fleet and forts on the Min River.

The French ships in front of the Foutcheou were the aviso *VOLTA*, the gunboats *LYNX*, *ASPIC* and *VIPÈRE*, the cruisers *DUGUAY-TROUIN*, *VILLARS*, *D'ESTAING* and small torpedo boats hull number 45 and 46. These nine vessels were equipped with 58 guns, of which five of 190 mm, 47 of 140 mm and six of 100 mm

and a number of revolver-guns. The cruiser *CHÂTEAURENAULT* and aviso *SAÔNE* were in surveillance at the mouth of Min River, between the fairway Mingam and Kimpai, having the mission to monitor Chinese movements and to prevent the passage of ships. The Admiral was onboard of cruiser *TRIOMPHANTE*, but he did not have the certainty that the ship, whose draught was 7 meters, was able to navigate upstream on the river.

To the French ships gathered in front of the port of Foutcheou, the Chinese could oppose four cruisers, five avisos and three gunboats, armed with a total of 47 guns, two of 250 mm, one of 190 mm, 19 of 160 mm, and 25 of smaller calibre. Also, there were 11 war junks armed with cannons, seven steam boats carrying torpedoes and a large number of ships loaded with explosives. These forces were supported by numerous land troops, seven batteries of artillery, some of which were of recent production, the French ships being in there area of the shooting.

Thus, on 23 August, after he received the approval of the Viceroy, Admiral Courbet triggered the military action. While the torpedo boats 45 and 46 attacked the Chinese cruisers *YANG-OU* and *FOU-SING*, all the other French ships opened a fire raging on the objectives that they had settled. The cruiser *TRIOMPHANTE* appeared later on by managing to navigate upstream on the river. Due to its strong artillery, it participated in the action from distance.

After 40 minutes of fighting, the Chinese squadron ceased to exist. Apart from two small gunboats which, due to the small draught, were able to escape upstream, all the other Chinese ships were sunk or beached in the flames and abandoned, while French ships were almost intact. At this stage, the fire was directed against artillery batteries installed on both riverbanks, which were silenced after 16 hours. The French victory was complete. The Chinese lost about 2 000 people, while the French had six dead and 27 injured.

The Admiral led the ships to a new anchor position, outside of shooting distance of forts guns, to spend the night. It was a night of alert, during which ships were many times required to carry out manoeuvres in order to avoid the vessels loaded with explosives released downstream by the Chinese. The next day, the Admiral executed a systematic bombardment of the arsenal.

His mission was thus almost finished at Foutcheou, remaining just to complete the last part of his instructions, to destroy the forts on the River Min. The Admiral transferred his flag from *VOLTA* to *DUGUAY-TROUIN* and then, on 25 August, he left the anchoring area. He had to confront 137 guns with calibres ranging between 60 and 210 mm scattered into numerous batteries on both banks of the river. Artillery pieces of 210 mm were arranged in pillboxes and armour sites.

Using a streamlined method, the Admiral attacked each enemy position, as he approached it. *TRIOMPHANTE* and *DUGUAY-TROUIN*, with their heavy artillery, neutralised, one by one, the unprotected guns, and the other ships, with the 100 mm artillery, completed destruction. Then, marine infantry companies were landed, completing the destruction of the Chinese artillery, and then returned onboard. During the night, the Admiral dispatched his squadron in an anchoring area uncovered by the enemy artillery, and next morning he resumed the work.

For three days, all the fortifications were bombarded and transformed in ruins. On 29 August, Admiral Courbet came out triumphantly, with all vessels on the Min River, the French losses being insignificant.

However, the effect produced on China by the Foutcheu battle did not have a major effect on the situation. Admiral Courbet again insisted to operate in the North, closer to Beijing and the Chinese Government, wanting to be allowed to go to Che-Fou, where he would establish the basis of operations, then the troops would be transported to occupy, at the same time, Wei-Hai-Wei and Port Arthur. The French Government denied the plan, insisting on the first approach, namely for Keelung Harbour and the coal supply to be seized, as a form of pledge.

Admiral Courbet was ordered to act with all his forces against the port of Keelung, being supported by a detachment of 1 600 marines and artillery, carried by vessels *TARN*, *NIVE* and *DRAC*.

Despite his reluctance in connection with the success of the operation ordered, and his persistence regarding his preference for an intervention in the Gulf of Petchili, Admiral Courbet received directions from the French Government to head to Keelung and Tamsui.

To execute this order, the troops were landed in the morning of 1 October, in Keelung, being supported by the *DUGUAY-TROUIN*, *BAYARD*, *CHÂTEAURENAULT*, *LUTIN* and *SAÔNE*, while Admiral Lespès, with *LA GALISSONNIÈRE*, *TRIOMPHANTE* and *D'ESTAING*, conducted a diversion at Tamsui to retain Chinese troops and prevent them from moving to Keelung to enforce the defence there.

Chinese resistance at Keelung was relatively weak, due to the effectiveness of artillery fire of the warships, Chinese troops retreating gradually behind the hills. On 4 October, the operations were completed. However, it was evident that the number of troops landed there were not enough to conquer the coveted coal deposits and also, conquered positions would not be preserved if Chinese forces were not prevented from being supplied and supplemented through the neighbouring port of Tamsui.

Thus, that port had to be conquered, the mission being assigned to Admiral Lespès. Unfortunately, it was impossible to provide him with the infantry battalion

he had requested, because keeping the positions at Keelung required all the available land troops. In these circumstances, actions against Tamsui were triggered on the morning of 8 October with only one landing company, on a difficult terrain, where the naval artillery support could not be carried out effectively, but only at a small distance from the shore. For such an action, a larger force should have been assigned, with a cohesion and professionalism that the landing company did not have. The operation was completed, under these conditions, with a severe failure. The marines were rejected with violence, with considerable losses, and could be recovered only by the intervention of brave Lieutenant Boué de Lapeyrère, commander of *VIPÈRE*, who came quickly with his ship close to the beach, managing to keep away the Chinese.

At the Government's order, Admiral Courbet blockaded the West coast of Formosa, starting of 23 October, an action that asked for six months of exceptional efforts on behalf of ships, crews, and commands, without any result. Winter had arrived, and the French ships were subject to violent storms, along a coast that offered no place to shelter. Although the number of ships increased little by little to 30, of which five battleships and 14 cruisers, that number was insufficient to ensure an effective blockade on the entire length of the coast. This blockade, called "*peace blockade*", because it was run without a declaration of war, was more an illusory one, because it was unable to prevent the infiltrations of Chinese reinforcements on the island. Due to those reinforcements, the Chinese army on the island grew progressively, from 5 000 men, in September 1884, to 30 000, in January 1885.

While the occupation troops at Keelung, after receiving reinforcements, was able to broaden, to some degree, its positions, and the French warships were maintaining the blockade, Admiral Courbet had suddenly, in February 1885, the opportunity to conduct a brilliant and fruitful naval action. Learning that Admiral Ting left Shanghai with three steel hull cruisers, a frigate and a corvette, Admiral Courbet transferred the command of blockade to Admiral Lespès and started looking for Chinese vessels with *BAYARD*, *TRIOMPHANTE*, three cruisers, a gunboat and an aviso. The enemy was discovered after five days of surveillance, on 12 February, at 05.30. Unfortunately, the Chinese ships could travel easily with 15 knots, while the French fastest ship, *BAYARD*, could reach only 12 knots. As they were in the high seas, nothing prevented the Chinese from getting away. The frigate *YU-YEN* and corvette *TCHEN-KING*, unable to follow the big Chinese ships, headed for the coast and took refuge in the port of Sheipoo, where fairway was unusable for French warships.

The two Chinese ships were considered safe and began to celebrate, quietly, the first day of the year, which, for the Chinese, started on 15 February,

when they were suddenly attacked in the anchoring area, on the night of 14 to 15 February, by two steam engine boats carrying torpedoes, led by Captain Duboc and Lieutenant Gourdon. While the frigate *YU-YEN*, hit by two torpedoes, began to sink, the gunners onboard and two batteries of field artillery also opened an uncoordinated fire. In the excitement, they hit corvette *TCHEN-KING*, which began to sink as well. After they spread on unknown channels, the two attacking boats were able to return to the *SAÔNE*, next day in the morning, losing only one man.

The French Government recognised that the action directed against Formosa did not have any influence on the attitude of the Chinese leadership, and authorised Admiral Courbet to ban the annual maritime traffic of the stored reserves of rice in the South provinces to Northern China.

The Port of Shanghai being the main load centre, Admiral Courbet ordered that a significant number of vessels were maintained, starting 4 March, at the mouth of the Yang-Tse River, in order to block the vessels transporting rice. At the same time, the Admiral blocked, at the entrance to the Ning-Po River, the three Chinese cruisers which escaped on 12 February.

Formosa blockade proving ineffective, the Admiral suggested the French Government to capture the Pescadores Islands, easy to occupy and defend, rather than to continue an action without solution along the coast of Formosa. This mission was approved, so that the French fleet, consisting of battleships *TRIOMPHANTE* and *BAYARD*, cruisers *D'ESTAIGN*, *DU CHAFFAULT* and a transporter, *ANNAMITE*, loaded with landing troops, was in front of the port of Makung on 29 March 1885. The five forts, armed with 27 guns, covering the entrance to the port, were silenced after a methodical but short bombardment. The troops were landed on the coast and advanced quickly under the protection of the artillery on cruisers and gunboat *VIPÈRE*, which arrived later in the area of operations. The next morning, all ships entered the port of Makung, while the infantry and landing companies continued the land operations. Occupation of the entire Makung Island was completed on 1 April 1885, with minimum French losses.

Although the port had a very well-sheltered bay, providing an excellent naval base for French naval forces, its conquest came too late. After a few days, on 4 April 1885, a preliminary peace treaty was signed, followed, on 9 June, by a final *Treaty of peace, friendship and commerce*, under which China relinquished all its rights over Annam and withdraw the army from Tonkin. On the other hand, France had to evacuate Formosa and the Pescadores within one month after the signing of the Treaty.

The mission of Admiral Courbet was thus complete, with nothing else to do but to prepare the evacuation according to the peace treaty, activities which were

carried out with his well-known consciousness and precision. Nevertheless, tiredness and worries generated by this campaign of retaliation, much too complex and disappointing for a great military commander, had shaken the health of the Admiral, who died on 11 June 1885, in the Bay of Makung, onboard cruiser *BAYARD*.

Naval Actions during Franco-Siamese War

The Kingdom of Siam was looking spitefully as French dominance stretched over Cochinchina, Cambodia, Annam and Tonkin. Its attitude was encouraged by the British diplomacy and the indifference of the French Government, and by the uncertainty of border control. As a result, little by little, Siam stepped into the territories that undeniably belonged to the Kingdom of Cambodia or the Emperor of Annam. In early 1893, that advance had reached the Mekong River on a large portion and in some areas even exceeded, Siamese outposts being installed at a distance of 40 kilometres from the capital of Annam. Dizzy with success, the Siamese leadership and their agents started to behave in an arrogant manner; the incidents multiplied, and the situation became intolerable. Under pressure from Parliament, the French Government decided, in early 1893, to take the necessary measures to safeguard the rights of its protégés and rejected the Siamese outposts to the West of Mekong River by a peaceful action.

When the French troops got close, the Siamese evacuated without any resistance the majority of the outposts that they had settled on the left bank of the River. Nevertheless, in early May, they attacked and destroyed a French detachment, and on 16 June 1893, they massacred a French official and his escort.

The French representative to Bangkok, Auguste Pavie (1847-1925), was instructed to claim compensation for these acts, which constituted a serious violation of human rights. In front of the hesitations shown by Siam, the French Government ordered Rear Admiral Edgar Humann, the Commander of the French naval forces in the Far East, to send two warships to Bangkok, where the gunboat *LUTIN* was already in place. The aviso *L'INCONSTANT* and the gunboat *COMÈTE* were assigned for the mission. The commanders of the ships were instructed not to show any animosity, but only to support the actions of French minister and to protect the French citizens.

The instructions given to Captain Bory, the Commander of aviso *L'INCONSTANT* and Commander of the French naval group, directed that the group was not supposed to open hostilities, but to be able to respond to force by force. The two warships started their journey on 10 July and arrived in front of the breakwater of Meinam on 13 July, around 18.00.

In the meantime, the Siamese Government asked urgently that those ships would not be headed for Bangkok. In the spirit of reconciliation, the French

Government accepted. Vice-Admiral Humann and French Minister of Siam agreed, in a telegram on 13 July, that the ships should stop behind the breakwater in front of Meinam.

Unfortunately, those new instructions did not arrive on time onboard *L'INCONSTANT*. When *L'INCONSTANT* arrived in front of Meinam, the Commander was greeted by Auguste Pavie, who did not release the new provisions, informing him just about the fact that the Siamese Government did not authorise the passage for the French warships. Instead, he received a copy of a telegram sent by the Admiral, on 12 July, to the French Minister, through which he insisted on the need for a vigorous interventions as a response to the Siamese procrastination. However, those messages did not direct to force the entrance. On the contrary, the Admiral indicated that, if the Siamese opposed to the passage of ships, the French warships should perform the legal summons.

The situation was as follows: behind the dam, there were nine Siamese warships, armed with a 210 mm gun, four guns of 150 mm, nine of 120 mm, 28 of 100 mm, six of 80 mm and a considerable number of smaller guns and machine guns. *L'INCONSTANT* and *LUTIN*, small ships with wooden hull, had only five guns of 140 mm and three of 100 mm. The French ships had to pass the breakwater, then a barrage and, in the end, to pass along the Siamese warships and three forts, two of which were equipped with nine guns and the other with eight guns of 210 mm displaced in armoured turrets. The disproportion of forces was enormous. However, Commander Bory was a brave and energetic man, animated by a high sense of devotion. The instructions seemed clear. Slave of the order, he had no time for hesitation. Preceded by a small French trading ship, *J. B. SAY*, *L'INCONSTANT* passed the breakwater with determination, followed by *COMÈTE*. One of the forts opened fire immediately, without summon or notice. The French ships were not fighting back until after the twelfth volley. Passing *J. B. SAY*, which was destroyed, *L'INCONSTANT* engaged onto the narrowest side, surpassed the barrier and went away from Siamese ships using the existing landscape on both sides of the channel. The latter had also opened fire at the same time in trying, in vain, to force the French ships to enter the naval mine barrage installed on the fairway.

L'INCONSTANT and *COMÈTE* broke through without hesitation by firing with all the guns onboard. After a very strong commitment, which lasted only a few minutes, they overcame the enemy ships and came outside their radius of action, with minimum damages and losses. On the contrary, the Siamese ships suffered heavy losses, three of them being forced to run ashore to avoid sinking.

The French ships continued their way, firing upon the last fort. At 21.30, they met *LUTIN* in Bangkok and anchored in front of the French legation.

The sailors hoped that their success would be exploited without delay and they could be deployed in front of the Royal Palace to demand the surrender of the fleet, as well as the evacuation and destruction of batteries that attacked disregarding the rules of international law. Nevertheless, diplomatic reasons did not allow such a thing; the French Minister in Siam was invited to give immediate explanations on the ambush committed against French ships. The latter were ordered to open fire only in case of attack or imminent danger.

Then, on 18 July, the French Government gave the Siamese Government an ultimatum in which it summarised all the claims. In the absence of a response or in case of refusal, after 48 hours, the French Minister would leave Bangkok and a blockade would be immediately declared on all the Siamese coasts. The Siamese Government was warned that immediate retaliation would be displayed if any act of hostility would be committed against the French ships leaving Bangkok for Meïnam.

The French Minister delivered the ultimatum to the Siamese Government on 20 July, and the answer came on 22 July, at the right time, but it did not satisfy the French demands. Therefore, Auguste Pavie left Bangkok in the afternoon of 25 July, as well as the warships *L'INCONSTANT*, *LUTIN* and *COMÈTE*. On 29 July, Admiral Humann declared the blockade on the Siamese coasts, which was executed by *TRIOMPHANTE*, *FORFAIT*, *L'INCONSTANT*, *COMÈTE*, *LION*, *LUTIN*, *VIPÈRE*, *ALLOUETTE*, *ASPIC* and two torpedo boats that were part of Saigon defence.

Not supported by England, as would be expected, the Siamese Government agreed, after a few days, to the conditions of the ultimatum.

On 5 August 1893, Vice-Admiral Humann gave the order for the blockade to be lifted, and the Far East squadron resumed peacetime activities.

BIBLIOGRAPHY

1. B. Elleman, *Modern Chinese Warfare, 1795–1989*, Penguin Books, New York, 2001.
2. Eugene Germain Garnot, *L'expédition française de Formose, 1884-1885*, Payot, Paris, 1894.
3. L. Huard, *La guerre du Tonkin*, Paris, 1887.
4. Martin Stuart-Fox, *A History of Laos*, Cambridge University Press, 1997.
5. Patrick J. N. Tuck, *The French Wolf and the Siamese Lamb: The French Threat to Siamese Independence, 1858-1907*, White Lotus, 1995.
6. A. Thomazi, *La conquête de l'Indochine*, Payot, Paris, 1934.

THE “SECRETS” OF THE SUCCESS ON THE SECRET FRONT

Colonel Daniel MELCIOIU

The article discusses some aspects related to the relationships between Eugen Cristescu and Mihail Moruzov, two heads of secret services in Romania, helping us understand two concepts diametrically opposed regarding the mission and practices of the state security services, in a period that was extremely important for Romania's history, namely the one between the 2nd and the 5th decades of the last century. Although relatives by marriage, Eugen Cristescu and Mihail Moruzov were rivals professionally, not only because of the excessive pride characteristic to policemen, but especially because of their different views on the mission of the services they led at that time. While Eugen Cristescu was a justice fighter who militated for the strict observance of the laws related to police and security forces work, Mihail Moruzov – a self-educated person par excellence – considered that the secret service deserved everything and, therefore, it was allowed everything.

Keywords: intelligence service; Mihail Moruzov; Eugen Cristescu; counterintelligence; management

The history of the 20th century has proved that it is worth the risk of involving responsibly in the confrontation on the secret front, especially in the case of small and medium-sized countries. This is because, in most cases, there is little alternative to survive as a nation and state unless getting caught in this game! In essence, it is a permanent race of intelligences put to work to support the national, regional or global interests related to the stability of a system. It is a dispute in which all, absolutely all those involved have a chance. Small and medium-sized countries that had strong intelligence services – meaning that they were well equipped, judiciously organised and had highly qualified personnel – usually got an extra chance to promote defence policies before or at the negotiating table beside the great and rich ones, more precisely where political games were made, maps were drawn or areas of influence and interface were settled¹. The great empires known over time were not able to maintain without establishing an intelligence system. The victories of great leaders, from ancient times to the modern

Colonel Daniel Melcioiu – “General Nicolae Condeescu” Defence Intelligence Training School, București.

¹ Cristian Troncotă, *Duplicitarii. O istorie a Serviciilor de Informații și Securitate ale regimului comunist din România*, Editura Elion, București, 2003, p. 7.

era were preceded by intense intelligence activity to understand the forces and means available to the opponent. In support of the statement one can quote Napoleon Bonaparte: *“My military successes are said to be due to my genius; however, I will answer that they are the result of mathematical calculations based on accurate information”*. History teaches us that, above transient requirements and subjective interests, the common thread running intelligence continuity and tradition should be solidarity and understanding to serve Romania’s national interests.

The heads of secret intelligence services, through the regular contact with decision makers, both in political-diplomatic and military circles, as well as through agents selected from all places and environments, may become influential people in the state over time, which happened in too many cases. Some earned their position through personal merits and professional achievements, and others used most of the information made available to them. The influence a head of a secret intelligence service may have on decision makers depends on the political regime in totalitarian states, where there is a highly centralised intelligence structure, having mainly the role of political police so the power accumulated, in time, by the head of the institution is hardly hindered by laws and exuberance. Lavrenti Beria, in the USSR, Gabor Peter, in Hungary, and Alexandru Drăghici, in Romania, are just three examples in a series too large to be invoked.

In contrast, in countries with traditional democracy, there is usually an intelligence community consisting of several specialised structures, each in a specific area. The influence the heads of such institutions can exercise in democratic regimes is more limited by the legislative framework. However, history proves that, even in the case of the information community, one of the services usually plays the role of *“primus inter pares”*, the collaborative and cooperative relationships being able to transform, under certain circumstances, even in forms of control or subordination. In this context, it has become necessary to create systems to monitor the activity of intelligence services, systems belonging either to the executive, the legislative power, or the civil society, as stipulated by the legislative framework².

Mihail Moruzov

The first head of the Special Intelligence Service, Mihail Moruzov (12.04.1924 – 13.09.1940), was an intelligent man, showing remarkable talent for working in the intelligence field, but having a substantially lower education than the one required by the position he held, fact that strongly marked the way he led the service. Born in Zebil, a commune in Tulcea County, the son of a Lippovan priest,

² Cristian Troncotă, *Mihail Moruzov și frontul secret*, Editura Elion, București, 2004, p. 17.

he could speak Russian and Bulgarian, but could not speak any Western language, which resulted in great difficulties in his collaborative relationships. *“He attended three classes of high school, but he did not read any book except newspapers – and did it superficially. When he needed cultural knowledge, he addressed a specialist and memorised the information for reproduction. He did not like to write or even to sign. Thus, in the service archives, his resolutions are extremely rare, and he signed papers only when it was absolutely necessary”* – Eugen Cristescu critically stated about Moruzov³. Moreover, it is possible that the gaps in his education, combined with exaggerated caution, could be at the origin of his aversion – that has become notorious – to documents and in particular to those it was incumbent upon him to record resolutions or sign. The reason for this aspect is found in his character, because he did not like to engage in any formal action to always have the ability to evade responsibility. In fact, the service problems were resolved verbally and so were issued the necessary orders and provisions. He entered the Secret Service in Dobrogea when he was very young, during the First World War, and he became the head of the service. After the war, he was in conflict with Romulus Voinescu – Inspector General of Police Services, because of earlier misunderstandings, which would eclipse the careers of the two. The dispute was based on the envy aroused because of the success achieved by the service led by Mihail Moruzov. Thus, the local representative of the General Security sought to compromise even the measure taken by the military to directly control the service. Specifically, in April 1918, the General Security accused Moruzov of collaborating with German and Bulgarian espionage, of favouring the revolutionary troops, and of having links with Tsarist espionage. The Great General Headquarters ordered an inquiry in this regard to be carried out by the military. The results of this investigation *“swept”* all the allegations made by the General Security. Moreover, the service led by Moruzov was thanked for the way it carried out its activity⁴. However, the tactic of getting in touch with everyone, reaping each and every possible benefit, preventing unwanted events for the Romanian armed forces, as well as of avoiding unnecessary loss of life was much appreciated by the Great General Headquarters. The scale of the conflict between Romulus Voinescu and Mihail Moruzov resulted in the two being called before King Ferdinand. He asked both of them to get reconciled and to further work together for the public good, in the name of supreme interest⁵.

Recommended by General Constantin Dragu and by Colonel Mircea Rădulescu – the chief of Section II of the Great General Staff, in 1924 he succeeded in being

³ *Din memoriile lui Eugen Cristescu*, 1968, p. 6.

⁴ Colonel Nicolae Meianu, *Istoria serviciului secret de informații al armatei române*, București, 1973, p. 55.

⁵ *Ibidem*, p. 80.

appointed head of the Secret Service, which was newly established within the Ministry of War. Romulus Voinescu strongly opposed to this appointment, but the Great General Staff did not take account of it, aspect that subsequently affected the cooperation between the General Security and the newly-established secret service. But why Mihail Moruzov??!!

Mihail Moruzov was also appointed to organise a military secret service in 1913⁶. On this occasion, Mihail Moruzov made an extremely professional statement according to which: “*An intelligence service cannot be improvised*”.

Here are some of the facts that recommended Mihail Moruzov to be called to organise a secret service by the Great General Staff officers who knew his activity in the First World War. In 1917 (when he was 30), he headed the *Delta Security Service*. A turbid atmosphere prevailed at that time. Romania, which just entered the war, received blow after blow. Bulgaria, allied with Germany, troubled the waters hoping that it could seize the entire Dobrogea, while the Russian troops, our allies, under Bolshevik influence, did not really feel in the mood for fighting, waiting for the revolution that, on 25 October (7 November), would lead to the establishment of the Bolshevik regime. His confident and courageous manoeuvres over these troubled waters, proper to a true son of the Delta, helped Mihail Moruzov and his Service to categorically influence the fate of the fights on this front:

- by an action conducted 78 kilometres in the depth of the enemy territory, Moruzov captured the head of the German intelligence service for the area of Dobrogea;
- he arrested 156 out of the 178 German spies sent in the area;
- he insinuated himself in a delegation of the Russian Army that was to negotiate the surrender of two Russian divisions to the Germans, and prevented the conclusion of an agreement until the Romanian Command managed to inform the Allied Command;
- he took the lead of a Red Army division in the area, subsequently dissolving it;
- he organised the purchase of the Russian fleet on the Danube for two million lei and only a hasty attack on it prevented the completion of the action;
- after the end of the war, he uncovered an action of the Russian intelligence services that planned to undermine the Romanian economy, throwing 12 million fake rubles on the market (to create a climate of trust, the first million was good. Moruzov received the million, transferred

⁶ *Ibidem*, p. 70.

it to the state budget and then stopped the action meant to invade the Romanian market with counterfeit money).

Without being accused of promoting empiricism in the activity of the service, he did not militate for the accreditation of scientific methods. It was obvious that Moruzov gave excessive credit to flair, inspiration and ingenuity, which he used to fill the gaps in education, as well as that he employed rudimentary methods or no method at all. Although he did not get used to reading, he was smart enough to assimilate the data he found interesting from others, and then to reproduce them as his own knowledge. Moruzov had no political or professional culture, except some practical knowledge, gained either through experience or through his relationships with more educated police or intelligence officers. According to the statements of Eugen Cristescu, *“with their help, either by pleading or by payment, a study on whatever problem was developed, and Moruzov retired to a villa in the Prahova Valley to memorise it. Thus, by this method, for those who did not know the background of intelligence problems, Moruzov appeared a <well informed man>, but as soon as he was forced out of the line established by him, he came with generalities and vague ideas, appearing as he was in reality – a unilateral man”*⁷.

Another system permanently cultivated by Moruzov, according to the critics of his activity, was to calculate and forecast the governments to come at the helm and the generals to head the Ministry of War and the Great General Staff. He informed all of them preventively, kept in touch with them, and even provided different personal services or benefits to ensure further relations. For example, when the Chief of Staff was inconvenient – as in 1934, when General Antonescu, as the chief of staff, demanded to know how the intelligence funds were spent – Moruzov moved the service at the Ministry of War and returned only when there was a chief of staff who agreed him. He was very cunning, secretive, always working with a small group of people. He always had confusing and complicated conceptions, but enough ability to handle the most complex situations. Mihail Moruzov distinguished himself due to his insight, orientation, vocation for intelligence work, experience, and effort, managing to make the Special Intelligence Service one of the most vigorous repressive bodies of the state. Being concerned with the problem of maintaining and strengthening his position, threatened by ongoing political instability in the country life, Moruzov adopted a flexible attitude towards the various reactionary groups engaged in the struggle for power, supporting them or, on the contrary, acting against them, depending on the chances of success. An argument to support this view is represented by the confidences

⁷ *Din memoriile lui Eugen Cristescu*, p. 29.

shared by Robert Bishop, officer in the Strategic Operation Services, who came to Romania with the US military mission, immediately after 23 August 1944, and consulted many Secret Service files regarding the Soviet Russia. The US officer made the following remark regarding these files: *“they contained the greatest collection of data regarding the Soviets from all over Europe, except for the files found in Germany. They presented a continuous data collection starting with the First World War. These documents reflected the work of many branches of Romanian intelligence services. However, the most important secrets were mostly obtained by a man and the agents managed by him. The experts who knew his work considered him the greatest spy who ever worked for Romania. He had over 200 active agents in Russia both before and after the war and there was no part of the country, including the Urals guarded area, not penetrated by him”*. As in addition, Ștefan Enescu, Moruzov’s secretary also remembered that *“the information obtained by the Secret Service went as far as to disclose what was discussed behind closed doors in the Council of People’s Commissars (government) of the SSR of Moldova”* – over the Dniester – *“which was a hub of the USSR against us”*. Mention should be made that Mihail Moruzov was the first head of the Secret Intelligence Service whom Admiral Canaris met directly and with whom he had most contacts, totalling four, two in Bucharest (in December 1939 and March 1940), one in Germany (April 1940) and another in Italy (3-5 September 1940).

In one of the rare documents preserved, with the handwritten signature of Moruzov, he explains in 1939: *“the Armed Forces Secret Service is the work of the undersigned, and it has taken a long time to achieve it. I can have only full satisfaction that, after 24 years of continuous efforts, during which I received no breaks, not even the legal one month per year, this constructive achievement provides a real service, relevant to the needs of the state armed forces. Our work is now imitated by Bulgaria, Hungary, Czechoslovakia, Poland, Russia, to which France will add soon. I do not speak about England, from which I inspired myself. It is necessary to stress that France made great efforts to establish an intelligence service on the Eastern Front, sending Captain Cury, an excellent intelligence element, but, because of the lack of the technical element, he had to give up the action. I highlight with real satisfaction that, exceptionally, so many officers from Section II were awarded the Legion of Honour, even the former captain Moraru, except myself of course, as I retired from that honour, not to have any obligation, even moral, to anyone, despite all the offers made”⁸*.

The secret of Moruzov’s success, according to those who appreciate his work, was that he was not involved in politics, he had no political beliefs, and he did not join

⁸ Mihail Moruzov, *Expunere asupra serviciilor de informații ale armatei*, SRI Archives, fund „d“, file no. 8097, pp. 6-12.

any political party. He did not sympathise with any politician of the time. *“He was seen by some as a kind of chameleon, because he immediately adapted to any situation, striving at the same time not to be at the whim of politicians, and to prevent the activity of the service he headed from being influenced by the government changes. As a result, he followed his belief undisturbed, not serving any government while working with all of them, acting unscrupulously, having the ability to identify and recruit capable people, whom he then rewarded generously for their work”*⁹.

We appreciate that the concern for staff training (*appendix 1*) is an aspect that is worth mentioning. *All these facts have resulted in a series of improper aspects within the service, having considerable negative consequences on the intelligence capability*, critically assesses Eugen Cristescu in his memoirs¹⁰. This attitude determined Moruzov, inter alia, after a period of deliberate hostility against the Guard members, to flirt with them, but many of the prominent elements of the organisation, headed by Constantin Maimucă – Director of Security Police and Colonel Ștefan Zăvoianu – Prefect of the Capital Police, having strong resentment against him and also considering him a formidable potential menace, preferred – despite the special attachment shown by Moruzov to Horia Sima and other Iron Guard commanders – to get rid of him. Furthermore, the relationship between Mihail Moruzov and Horia Sima was a very “*special*” one. Thus, under the crypto-name “*Professor Georgescu from Lugoj*” the legionary head was recruited by “*visionary*” Moruzov when he was just a young legionnaire desiring to accede to the top of the Legionary Movement. *“Horia Sima was recruited under threat of unmasking his secret collaboration with the German intelligence services, which explained the anathema, arrest and assassination of Moruzov during the ephemeral legionary government”*¹¹. In consequence, on the night of 27 November 1940, Mihail Moruzov was killed in Jilava, together with many dignitaries and police officers who acted against the Iron Guard members.

Immediately after Moruzov’s arrest, Marshal Antonescu, who actually ordered his arrest on 5 September 1940, appointed as head of the Secret Service an army officer, Colonel Nicolaid, whom he knew from the Great General Staff and the School of War, where he was an eminent officer. Colonel Nicolaid was a great theorist in intelligence, but he had no active practice in any institution with such a mission. As for his temperament, he was a slothful person who allowed his subordinates to work, limiting his work to signing the papers submitted to him and reading information bulletins. These features of Nicolaid actually mirrored in the activity

⁹ Paul Ștefănescu, *Istoria serviciilor secrete române*, Editura Antet, 2007, p. 63.

¹⁰ Aurel Rogoian, *Fereastra serviciilor secrete*, Editura Compania, București, 2011, p. 211.

¹¹ *Din memoriile lui Eugen Cristescu*, p. 6.

of the service he headed for ten weeks. During Nicolaid's leadership and based on Antonescu's orders and instructions, the "*Decree-Law on the establishment of the Special Intelligence Service*" was issued. Published in the Official Gazette of September 1940, during the first days of Antonescu's government, it marked the importance and urgency attached to the organisation of the service. General Antonescu intended that the service should not circulate between the Great General Staff and the Ministry of War, as in the days of Moruzov, never indulge in political games according to its head interests, but should follow the state policy, thus depending on the state leadership, organically exercised by the Presidency of the Council of Ministers. Nicolaid did not prove to be the right man to head the Secret Service because the few measures he took during the period he held that position were considered as being very shy and driven more by a desire to save appearances than to change the existing situation, so the revival expected by Antonescu regarding the activity of the service did not occur.

General Ion Antonescu was a military man with a rich experience, who honoured many of the command positions of the military hierarchy, until 6 September 1940, when he was appointed as Head of the Romanian state. He was aware "*that a state cannot be governed without having available an as wide and accurate as possible intelligence orientation*". There were occasions when he was directly involved in the intelligence activity by developing orders and regulations. Thus, for example, during 1922-1926, General Ion Antonescu served as military attaché of Romania in Paris, London and Brussels. Moreover, the Regulation on the organisation of the Romanian Armed Forces Secret Intelligence Service of 20 April 1934 was developed in a time when the general served as Chief of the Great General Staff, and the Regulation on the reorganisation of the same institution – on 31 January 1938 – came into force due to the same Ion Antonescu signature, but as Minister of Defence. All the mentioned aspects support the statement that Ion Antonescu was among those who knew how to appreciate the true role and place of an intelligence service for both the military and the whole modern society. From this perspective, one can also explain the fact that one of the first acts of government included the Decree-Law no. 3083 on the establishment of the Special Intelligence Service, which came into force on 8 September 1940, an event that marked the importance and urgency attached by General Ion Antonescu, as Head of State, to the organisation of such fundamental institution. By this Decree-Law the SIS was established, and a new phase in the history and tradition of intelligence in Romania started. The new intelligence service was established alongside the Presidency of the Council of Ministers and it was subordinated directly to the head of state. As far as the budget, logistics and administration were concerned, it depended on the Ministry of War

and the General Secretariat. As for the collection, verification and capitalisation on the information needed by political-military decision makers, art. 2 of Decree-Law no. 3083 stipulated that *“the SIS works with other ministries and the Armed Forces Great General Staff”*.

Eugen Cristescu

Ion Antonescu appointed Eugen Cristescu as head of the SIS. He was the director of the state administration and the personnel of the Ministry of Interior, and previously the director of the Security Police, known as a feared opponent of extremist political movements of the right and left – whose history recommended him as a man capable of bringing new life into the activity of the secret service, which he managed to do to a large extent, in the period 12.11.1940 – 23.08.1944, when he was in charge of the service. He had the energy and determination that lacked Nicolaid, and he was neatly superior to Moruzov as far as education was concerned. Moreover, his view was much more consistent with the requirements of the time regarding the activity that should be conducted by an intelligence service than the one of his predecessors.

After graduating the primary school in the village of Târgu-Ocna, he attended the Theological Seminary *“Veniamin”* in Iași, graduating it in 1916 with 8,56. The same year, he enrolled at the Law School in Iași but, because of the war, he interrupted his studies. He participated in the military campaign in the autumn of 1916, serving as health care sergeant. After the end of the war, he resumed his university studies, and six years after graduating he was awarded a doctorate in law at the University of Iași. After graduation, he worked for 14 years in the State General Security, and then, for six years, in senior positions in the Ministry of Interior. It was thus a rapid ascent, as he reached a high level in the professional hierarchy, from the deputy-chief of bureau to the one of general director. Besides the classical languages (Latin and Greek, he learned while attending the Theological Seminary), he could speak French and German very well, which facilitated the participation in numerous meetings organised in different European capitals on topics related to *“novelties and enhanced techniques in the police and intelligence activity”*. For a while, he was a member in the International Forensic Commission, representing the Romanian Police. As the head of the Security Service, and then deputy director and director of the Security Police, he contributed – as mentioned in a report –, *“to many operations and developments related to state security”*. In an annual professional assessment – *“qualification sheet”*, as it was called at that time – for the period 1 January 1927 – 1 January 1928, drawn up by the general director Romulus Voinescu, the following aspects regarding

his activity are mentioned: *“Official endowed with wonderful attributes for the chosen career. He has the necessary knowledge, sense of duty and sense of responsibility. Spirit of initiative; in achieving his tasks he proves goodwill, showing clear conceptions and profundity. Disciplined. Determination, integrity, loyalty. His behaviour towards the service and the public is respectable and civilised. Qualification: very good”*. The way the press of the time received the effectiveness of the State General Security – when Eugen Cristescu held the position of general director – can be illustrated citing an article in the newspaper *“Cuvântul”*: *“Fighting the difficulties that are inherent in current times, with personnel reduced to minimum, but able to do the duty at a cost of blood – there are numerous cases that prove it –, the State Security fully fulfils its mission”*¹². One of the most important sections of the Security was the one that monitored the activity of the communist movement. It was established due to the measures taken by Eugen Cristescu. The above-cited article commented on the efficiency of this section as follows: *“the State Security established a special section to monitor the communist movement and has managed to hand in to police a lot of agents and propagandists. It is one of the best organised services, and the GPU – from Moscow –, considers it the most important rival in Central Europe”*. Throughout his career as an official in the Ministry of Interior and the Presidency of the Council of Ministers, Eugen Cristescu was awarded six orders and two medals, and was penalised once, through a *“Decision of the Minister Secretary of State at the Department of Interior no. 70 632/6 on 9 November 1932”*. The document said that he was *“fined with the salary for a day because of insubordination”*. Unfortunately, it did not concretely explain what insubordination really meant. It seems that it was also insubordination that led to his change from the position of director of General Security to the one of inspector in the Ministry of Interior. In this regard, his brother, Gheorghe Cristescu, stated: *“Eugen was removed from Security as he refused to obey some illegal orders of the Camarilla”*. The truth is it was Mihail Moruzov – the head of the Secret Service that acted covertly to remove him from the leadership of the Security. The reason was the fact that Eugen Cristescu *“did not understand to engage in certain political interference of the Royal Palace and especially he refused to perform certain illegal and arbitrary arrests ordered by the Palace Marshal, in a game meant to divide the parties”*.

Eugen Cristescu’s activity as head of the service can be appreciated as a very complex and prestigious one. Thus, starting from the aspects regarding the need for personal files for the employed personnel, continuing with the regulation of the employment, assessment, advancement and remuneration of the personnel,

¹² The journal *Cuvântul* on 6 November 1933.

banning membership of any political party or participating in political activities, complying with keeping the service secret, establishing a credit and mutual benefit fund, reorganising the intelligence section – through a “*surgical operation*”, as Cristescu himself appreciated¹³, restructuring the counterintelligence section, entering into legality regarding the logistic activities performed by the service – especially financial operations, represented only a part of the directions for action established by Eugen Cristescu in his attempt to set up a modern intelligence service. His appointment as head of the Special Intelligence Service resulted in the service radical reorganisation, covering all its components, one of the adopted measures being the establishment of the preparatory school for intelligence agents (*appendix 2*).

We appreciate as eloquent the dialogue between Ion Antonescu and Eugen Cristescu, in the presence of Horia Sima and the Under Secretary of State Alexandru Roșianu (who proposed him to be appointed as director of the special intelligence service), on 15 November 1940, at Mogoșoaia station: “*You are not involved in any politics but the one of the head of state*”¹⁴. The obtained results were according to the trust and attention related to the service. Thus, statistics in 1941 reveals the following situation: the Special Intelligence Service attention was focused on 194 persons suspected of espionage or treason, out of which 85 in favour of the Soviets, 90 in favour of Hungary, 6 in the service of Bulgaria, 12 in the service of Germany, and 1 case of British espionage. During the same year, 300 people were convicted of espionage/treason. Mention should be made that the treatment applied to the members of the British-French espionage networks (R. Georgescu, I. Popovici, Alexander Eck, Nicolae Țurcanu, A.G. Chastelaine, I. Porter and S. Meșianu) and the Polish ones was a benevolent one, none of them being handed in to the Germans, despite all the pressure in this regard, and the prison conditions allowed going to the restaurant or going by car around the capital city. Moreover, there was a permanent collaboration with the German Army Intelligence Service, both on the front line and in the country. However, the interference of the few espionage agencies under the influence of the German Legation, Gestapo, SD and others, which acted illegally on the Romanian territory, required for their actions to be “*covertly*” monitored, to avoid some events that could severely affect the Romanian state. For example, the German project regarding the extermination of all the Jews in the capital and the main cities of the country during only one night was unveiled, so the idea was abandoned.

¹³ *Din memoriile lui Eugen Cristescu*, p. 54.

¹⁴ *Ibidem*, p. 42.

Eugen Cristescu's concerns were focused on the issues of coordinating and ordering information at national level. Thus, following his initiative, it was established, alongside the Presidency of the Council, a "Service to centralise information from all the intelligence bodies of the state", consisting of officers and civilian personnel specialised in this field. There the most important civilian and military informative bulletins and special reports were gathered, which were sent by the Great General Staff, Ministry of Interior, Foreign Affairs, War, Security, Police, Gendarmerie, Special Intelligence Service, Ministry of Justice, containing information obtained from prosecutors and prisons and, in general, any information from any authority or department that was considered interesting for the leadership of the state. Through the three reorganisations that took place in November 1940, January 1942, and April 1943, the SIS underwent profound structural, personnel, and design transformations, which entitled the statement that their initiator and creator, Eugen Cristescu, could be considered a true reformer by the Romanian intelligence history, a worthy continuator of the work started by his predecessor, Mihail Moruzov. The work of the Service reconstruction was initiated and carried out under the pressure of internal and international political events. With regard to the first reorganisation, a novelty in the structure of the service was represented by the "Mobile Echelon", which went along the front line together with large operational units, thus providing the Great General Headquarters with information¹⁵. The "Mobile Echelon", as a structure, had a chief of the echelon, a working front apparatus, an agency with information centres located at the border, a technical team, a health team, one of sketchers, and a guard consisting of gendarmes¹⁶.

After his arrest on 24 September 1944, Eugen Cristescu was investigated by the Romanian authorities. On 12 October, he was taken by the Soviets along with Generals Vasiliu, Pantazi and Tobescu, Marshal Ion Antonescu and his wife, Maria, Mihai Antonescu, Gheorghe Alexianu and Radu Lecca, and they were taken to Moscow, coming back in the spring of 1946¹⁷. Eugen Cristescu lived the years of detention in Aiud, Dumbrăveni and Văcărești prisons, being investigated to be exploited as a database. Under those conditions, he developed his paper "The Special Intelligence Service Organisation and Activity", regarded as the first paper on the history of the Romanian secret services. After about 15 days of hunger strike, forgotten and forsaken by all, Eugen Cristescu died on 12.06.1950 in Văcărești prison¹⁸.

¹⁵ Ion Lissievici, *Amintirile unui fost lucrător în serviciul de informații al statului*, p. 21.

¹⁶ Stan Petrescu, *Arta și puterea informațiilor*, Editura Militară, București, 2003, p. 338.

¹⁷ Cristian Troncotă, *Omul de taină al mareșalului*, Editura Elion, 2005.

¹⁸ Paul Carpen, in the journal *Vitralii*, no. 6/2011, pp. 75-81.

*

We consider useful to discuss some aspects regarding the relationship between Eugen Cristescu and Mihail Moruzov, as it helps us understand two diametrically opposed views regarding the mission and practices of the state security services. Although they were relatives by marriage, Eugen Cristescu and Mihail Moruzov were rivals professionally, not only because of the excessive pride characteristic to policemen, but especially because of their different views on the mission of the services they led at that time. While Eugen Cristescu was a justice fighter who militated for the strict observance of the laws related to police and security forces work, fact that results from historical documents, Mihail Moruzov – a self-educated person par excellence – considered that the secret service deserved everything and, therefore, it was allowed everything. Here should be mentioned the incorrect statement of Ivor Porter – member of the famous group “*Autonomous*”, parachuted in Romania by the British in December 1943 –, who, in his memoirs, presents Eugen Cristescu as Moruzov’s deputy. As we have already seen, up to November 1940, Cristescu worked only for the Security and as an inspector in the Ministry of Interior. Mihail Moruzov was the head of the Romanian Armed Forces Secret Intelligence Service for 15 years, the service being his exclusive creation. This aspect did not exclude the collaboration between the two, as it is commonly practiced between the police and secret services, which, maybe, confused the British diarist.

History proves, unfortunately, that, in Romania, secret services have always suffered the consequences of sudden political changes or blind struggle for power. What other relevant examples could be cited than those that the head of the SIS – Mihail Moruzov – and his deputy – Niky Ștefănescu – were shot by the legionnaires when they came to power, the next head of the institution – Eugen Cristescu – was sentenced to death by the communists, the sentence being commuted to hard labour for life, and finally ended, as other SIS officers, behind bars. And examples may continue, referring to more recently events. The history of Romanian intelligence and counterintelligence hides many names of known or unknown heroes, who never enjoyed the privilege of passing under the triumphal arches of glory. They did not enjoy the benefits of political change. Instead, they were to suffer the vicissitudes generated by such twists or unfortunate circumstances. And they had this fate perhaps because they were less fascist or anti-fascist, communist or anticommunist than others. They were the sons of the country. Nothing more to say.

Appendix 1

Mihail Moruzov was particularly concerned about the training of new personnel by the Great General Staff, either through courses organised by the Secret Service or through sending the best workers to get specialised in intelligence within the secret services of some European countries. Among those sent to specialisation was Cristescu – Eugen Cristescu's brother, old collaborator, former director of the Secret Service Photo-identification Department, then head of the General Security, who was sent to France with the specific mission to specialise in certain fields, especially in the modern organisation of an intelligence service. Cristescu was specialised under the direct guidance of some French specialists in graphics expertise, visible and invisible text expertise, legal identification, forensic and microphotography technique, being appointed, when he returned to the country, as director of the Photo-identification Department, which he organised following the French model.

Appendix 2

Thus, in his memoirs, Eugen Cristescu states that the head of state himself delegated a general to monitor the courses of this school established in April 1941, emphasising thus the importance attached to this field at the highest level. Out of the official documents¹⁹ regarding this structure organisation and functioning, approved by even the Presidency of the Council of Ministers, we find out that the “*SIS was the only body empowered to prepare the agents*” that were to perform their activity within all intelligence structures, namely: SIS, GGS, Gendarmerie, Police and Security. Four months were necessary for a series of attendees. The first series of agents was trained between April and June, and the second between September and December 1941. The courses started at 8.30 a.m. and lasted up to 12.30; they were resumed in the afternoon, between 16.30 and 18.30. The courses were structured in two modules. The first module lasted for 45 days, the subjects being related to professional general knowledge, and the second, which lasted for a shorter period of time, 30 days, was meant for practical training in the field. As specialties, three categories of agents were trained: *external undercover agents*, who were trained individually; *external uncover* for the cadres that were to hold positions as heads of intelligence structures, superior training; *recruiters*, a specialisation that required the attendees to have special qualities, taking into account the fact that it was an extremely sensitive

¹⁹ Cristian Troncotă, *Omul de taină al mareșalului*, op. cit., pp. 28-29.

but important activity for the intelligence activity. Among the selection criteria, and the qualities developed during education (training), the following were considered: adaptability to the environment and situations; ability to work hard; solid general knowledge. As far as the physical qualities are concerned, the course attendees *“had to show dignity and natural distinction, as well as the ability to easily exteriorise manners”*. Moral qualities were not omitted either. There were selected those who were *“self-confident and elegant, both in appearance and behaviour, calm under any circumstances, able to preserve their rank and position in society; physically and morally courageous doubled by a sense of duty, by firm consciousness and an exceptional sense of humanity; loyal and righteous”*. As far as the curriculum is concerned, there were the following common courses, attesting, at the same time, to the whole issues of intelligence activity: information technique in the field (8 hours – one day a week), terrorism and sabotage (20 hours), rightist politico-social trends (16), communism (20), irredentism (16), Jews, emigration, religious sects (16), freemasonry (4), legislation (40), intelligence and counterintelligence (34). There were also practical courses in the curriculum, such as: cipher (6 hours), signalling (14), laboratory information technique (30), intelligence and counterintelligence technique in the field (90), armament and firing (20). Other topics taught by both senior officers and civilian trainers paid per hour were related to make-up and disguise, currency of the countries of interest, interrogation technique (investigation of paratroopers, terrorists, saboteurs etc.). One hour per day was meant for sport sessions, within which the course attendees were trained in order to acquire some techniques and skills that were absolutely necessary in the intelligence activity, as follows: jumping, climbing, using white weapons, riding a horse, swimming, jiu-jitsu, driving and riding a motorcycle. The budget allocated to each series was 373 500 lei, out of which 60 lei per day for a course attendee and 300 lei per hour for a trainer (instructor). The courses taught by trainers and instructors prove extremely interesting as far as the theoretical aspects are concerned. Thus, for example, the themes related to *“General notions regarding the intelligence agency”* – lesson taught in intelligence and counterintelligence course – the following principles were mentioned: *“getting to know the psychological structure of the nation and the component social strata in the country where the action is to be conducted”*. It is also stated that the *“psychological structures often play a very important role in managing the agency”*, as *“the intelligence service does not work with objects or puppets but with people, so each man and every nationality have to be addressed in a specific manner”*. Certain *“national stereotypes”* were referred to, meaning that: *“the Russian citizen is mainly interested in adventure”*, while *“the Bulgarian one is interested*

in money". The Russian and Bulgarian patriotism" was considered "superficial" by the SIS trainers. With regard to the Hungarians, it was mentioned that "they are driven by a ferocious chauvinism, nurtured by clever propaganda" and that "for a Hungarian, expatriation is not a tragic aspect, as in the case of other people". As for the Jews that took part in the intelligence activity, the course attendees were told that they did not ask themselves "what they could lose" but "what they could win". There is certain subjectivity in these statements, which is obvious in the mention made at the end of the lesson, according to which "these conclusions are based on superficial observations". The recommendations for the work with the agency also prove educative: "the human resource you are to work with deserves attention and a thorough and profound study"; "man is not born a spy or an adventurer – the gifted person should be sought"; "the determining role in the intelligence activity is played by imagination, ability to adapt and talent of each and every person"; "a superficial person will have mediocre results, and a person with well developed mind resources will create new and exciting things"; "agents will be recruited among the intellectuals who are also good psychologists, knowing behaviours and being well educated, as they are able to assess". The course attendees also studied the "Guidelines regarding the agents' classification, recruitment and training". The normative act established the following structure of the intelligence agency: indicators, recruiters, residents and controllers. Courier, missionary, double and false agents were also used. For impersonal relationships, it was recommended the use of the "letterbox", following the example of the Soviet agents. Conspiratorial houses were the locations used by agents to transmit information and receive instructions. The last special aspect – speaking of 1940 – was represented by the course in disguise and make-up, practically exemplified by an expert of the National Theatre, within the same school. Because of the strain determined by the losses on the battlefield, the SIS training school ended its activity and, after the war, the promising start was abandoned, being preponderantly replaced by the Soviet experience and tradition.

English version by
✍️ *Diana Cristiana LUPU*

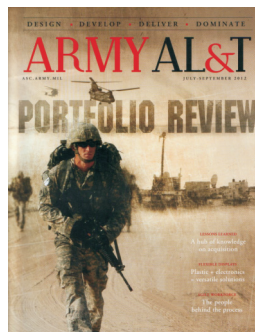
MILITARY JOURNALISTIC UNIVERSE

Armées d'aujourd'hui, France, no. 375,
November 2012

French-Saudi Cooperation Exercise *Tigre 2*, in Corsica • Demining NATO Exercise *Noble Mariner*, in Marseille Bay • Maritime Transit Group 519 • Engineer Corps Chief Corporal • Invitation to Public Debate for the Future Defence White Paper • Training Stage for Serving at High Level Command • Parliamentary Commissions: An Important Contribution to the Defence White Paper • Protection of Secret Documents in Defence Affairs • Multi-mission European Frigate (FREMM) – Technical Data, Systems, Capabilities • Harmonising Operational Aeronautic Maintenance • Intelligence Services in Operation (File)

Armées d'aujourd'hui, France, no. 376,
December 2012-January 2013

Aerial Operation *Volcanex* for the Evacuation of Residents from a Hostile Zone • A Night at Emergency Unit of Begin Military Hospital • Commando Instructor Up To the End • Russia and China in the Syrian Crisis: Blockage Reasons • Afghanistan – Disengagement in Highest Security Conditions • The Future Defence White Paper Will Define the Military Policy for the Next Twenty Years • Amphibian French-British Exercise *Corsican Lion* • Experts Behind the Green Berets • Joint Division of Infrastructure Nets and Intelligence Systems (DIRISI) in the Service of Forces • Cybernetic Defence – A Defence Priority • Events in 2012 (File)



“Portfolio” Perspective

• Demystifying the CPR • A Strong Lens • Maturing the Agile Process • Buying a Better Radio • A Measured Solution • The “New” Acquisition Workforce • Focus on the Industrial Base • CHEM DEMIL:

Mission Accomplished • Mission: MEDEVAC Recap • Logistics in Asymmetrical Conflicts • Flexible Communications • Closing a Security Gap • Communities of Practice • Cost Management Leaders • Keeping the Portfolio Profitable • Covering the Field • A Hub for Lessons Learned • DOTmLPP + dotMlpf = DOTMLPF • Sharing Services, Saving Money • Dollars and Sense • From the Director, Acquisition Career Management • A Process with a Purpose • Requirements Portfolios and the Joint Warfighter • Report from Afghanistan • Flight to the Future • Communication 101 • Myth Busting • The Long Road Home • Readiness at Best Value • Right-Sizing

Army Al&T, USA, October-December 2012

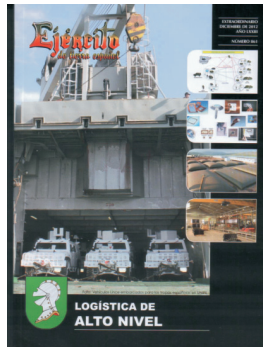
Planning for the Future • The Leading Edge • Building the Network Baseline • Top-tier Solution • Live Training Goes Mobile • Concealment Capability • Network Security, Smarter and Faster

- Birth of an Enterprise • Delivering Technology
- From Concept to Capability • Battery Power
- Higher. Farther. Cheaper • Army Refining Specs for Future Aircraft • Killing a Fly with a Sledgehammer • Innovation Marketplace • Not Just Fun and Games • Asymmetric Training • The Future of Counter-Ram • Advanced Protective Structures • Strength Through Sustainability • World-Class Workforce • Build. Nurture. Sustain
- A Framework for IT • Not Quite A Done Deal
- Breaking it Down • An Anthropological Eye on the Soldier • Quality Control, Close Up • The Power of LSS • Myth Busted • Getting Good data • Dollars & Sense

Ejercito, Spain, no. 860, December 2012

Difficulties in the North African Scenarios of the Arab Revolts • Military Profession: Due Obedience against the Obligation to Dissent • EUTM Somalia, the History of a Success • And Teddy Roosevelt Was Wrong

Capability Building within NATO and European Union through Multinational Cooperation: Operations Medical Support • BRILOG (Logistic Brigade) HQ CPX • A Bit of Thinking about Logistics • In-transit Visibility. Resources Tracking • MALE



(Army Logistic Command) Comprehensive Scorecard • COTS: Advantages and Disadvantages of its Presence in the Weapons Systems • The EMACON (Joint General Staff) Logistic Support Division and the Fuel Supply • Sustainment vs Logistic Support Maintenance Data: New Initiatives, New Logistic Solutions • From the Factory to the Forward B

Ejercito, Spain, no. 862, January-February 2013

Mali. The International Community Opportunity against T • Foreigner Soldiers. A Decade Serving Spain • File: Franco-Spanish Doctrine Seminar "DOCEX 12"

Foreign Affairs, USA, vol. 92, no. 1,

January-February 2013

Turkey's Moment: A Conversation with Abdullah Gul • The Fall and the Rise of the West: Why America and Europe Will Emerge Stronger from the Financial Crisis • Do Less Harm: Protecting and Compensating Civilians in War • Can America Be Fixed? The New Crisis of Democracy • The Life of the Party: The Post-Democratic Future Begins in China • Democratize or Die: Why China's Communists Face Reform or Revolution • The Mirage of the Arab Spring: Deal With the Region You Have, Not the Region You Want • The Promise of the Arab Spring: In Political Development, No Gain Without Pain • The End of Age of Petraeus: The Rise and Fall of Counterinsurgency • Barak's Last Battle: An Israeli Lion in Winter • Getting to Yes With Iran: The Challenges of Coercive Diplomacy • Pull Back: The Case for a Less Activist Foreign Policy • Lean Forward: In Defence of American Engagement • Rebooting Republican Foreign Policy • America's Misguided Approach to Social Welfare

Foreign Affairs, USA, vol. 92, no. 1,

March-April 2013

Generation Kill: A Conversation with Stanley McChrystal • Beyond the Pivot: A New Road Map for US-Chinese Relations • The Long Arm of International Law: Giving Victims of Human Right Abuses Their Day in Court • Gangster's Paradise: The Untold History of the United States and International Crime • Capitalism and Inequity: What the Right and the Left Get Wrong • Mexico Makes It: A Transformed Society, Economy, and Government • Breaking Up Is Not Hard to Do: Why the US-Pakistani Alliance Isn't Worth the Trouble • Japan's Cautious Hawks: Why Tokyo Is Unlikely to Pursue an Aggressive Foreign Policy • The Lost Logic of Deterrence: What the Strategy That Won the Cold War Can – and Can't – Do Now • The Evolution of Irregular War: Insurgents and Guerrillas From Akkadia to Afghanistan • Red White: Why a Founding Father of Postwar Capitalism Spied for the Soviets • Getting the GOP's Groove Back: How to Bridge the Republican Foreign Policy Divide • A Light in the Forest: Brazil's Fight to Save the Amazon and Climate-Change Diplomacy • Own the Goals: What the Millennium Development Goals Have Accomplished

***International Security*, USA, vol. 37, no. 2,**

Fall 2012

Two Concepts of Liberty: US Cold War Grand Strategies and the Liberal Tradition • Just War Moral Philosophy and the 2008-09 Israeli Campaign in Gaza • Israel's War in Gaza: A Paradigm of Effective Military Learning and Adaptation • The Psychology of Threat in Intergroup Conflict: Emotions, Rationality, and Opportunity in the Rwandan Genocide • China's Fear of Contagion: Tiananmen Square and the Power of the European Example • Debating India's Pathway to Nuclearization

***Jane's IDR*, UK, vol. 45, November 2012**

US Navy Leads Massive Middle East Counter-mine Exercise • British Forces Lay Down Air-land Integration Anchors • Details Emerge on US MPC Bids • Ukrainian Companies Combine to Develop Seeker for R-27 Missile • RUAG Develops Vehicle Robotics Kit • Singapore Gives M-346 New Lift • Russia to Field Fleet of New Armoured Fighting Vehicles • Let's Twist Again: German Tackles Tornado Fleet's Future Capabilities • Talking Hot Air: Hybrid Air Vehicle Development Proceeds Onwards and Upwards • Germany Faces Up to Forces' Future CIS Needs • Chinese Whispers: Anti-armour Weapon Development Quietly Achieves Self-sufficiency • Far and Away: Future Multimission Maritime Strike Missile Emerge • Planning and Preparation: New Air Operations Tools Leave Paper Trailing • Out of the Shadows: More Than Just a Workhorse • Data, Data Everywhere: Adrift on a Sea of Intelligence

***Jane's IDR*, UK, vol. 45, December 2012**

NATO Marks Successful "Live-Fire" Test for BMD Command and Control • Italian Army Aviation Fully Operational with NH90 • Japan, US Launch "Keen Sword" Exercises Amid Backdrop of Ongoing Regional Tensions • China Details Latest PLZ52 155mm Self-propelled Artillery System • Roboteam Rolls out UGV Family • France Completes D2AD UAV Sea Trials Phase • Hungary's ForcEi UAV Programme Bears Fruit • Altered State: UK Looks into Augmented Reality • NATO' ARRC: NRF Secures Approval from on High • DARPA Casts a Wide Net for Robotics Challenge • Sikorsky Looks to Expand X2 Technologies • Wagon Train: Forces Look to Logistics Lessons from Operational Deployments • WOLF in Soldier's Clothing: Soldier Systems in the AUSA Spotlight • Shot

and Shell: Sharpen Bundeswehr Armoured Training • View from on High: the RN's Crowsnest • Smart Thinking: 21st Century Technology Marks a New Era in Cockpit Upgrades • Homing in: VL MICA Seeks New Targets • Cultural Awareness Systems Help Soldiers Navigate Human Terrain

***Jane's IDR*, UK, vol. 46, January 2013**

GMLRS Utilisation Plateaus in Afghanistan • MEADS Completes First Intercept as Budget, Procurement Questions Loom • China Continues to Look to Russia and Ukraine for Aero-engines • Hungary Designs Indigenous Armoured Vehicle • L-3 CPS Develops M60 Upgrade • Rear View Mirror: HIS Jane's Looks Back on 2012 • Tactical Network Rover Targets RIPN Two-way ISR for JTACs • German Army Gears up for Global Leopard Tank Operations • Village People: Securing Afghan Communities From the Bottom up • Air Show China 2012 Opinion: More to Show – Less to Say • BAE Systems Poised to Kickstart CV90 Armour Family Production Line • 21st Century Warrior: Working Up the CSP • On the Prowl: Germany's New Helicopter Fleet Prepares for Afghanistan Operational Debut • On a Roll: Renault Trucks Defense Pushes Ahead with VAB Mk 3 • Blast Away: Reactive Under-belly Protection Systems Target IEDs • Bullseye: The Rise of Precision Land-based Weapons • Gazing out to Sea: Airborne Maritime Surveillance Radar Scan New Horizons • On the Horizon: Are the Next Generation of UAVs Ready to Take Off? • Iveco LMV Order Book Builds up • Flying Labs: From the Strange to the "Plane" Weird

***Military Review*, USA, vol. 42, no. 6,**

November-December 2012

The Right Way: A Proposal for an Army Ethic • Preventing Mass Atrocities in Sub-Saharan Africa through Strategic Engagement • Policy, COIN Doctrine, and Political Legitimacy • The Afghan National Army: Has the Capacity Building Become Culture Building? • Public Understanding of the Profession of Arms • Africa's Brain Drain: Its Impact on Security and Stability • Smooth is Fast: Managing Security Transitions for Enduring Freedom • Reframing Army Doctrine: Operational Art, the Science of Control, and Critical Thinking • Spectrum of What? • Seven Design Theory Considerations: An Approach to Ill-Structured Problems

Military Review, USA, vol. 42, no. 6,

January-February 2012

Empirically Based Leadership: Integrating the Science of Psychology in Building a Better Leadership Model • Building the New Culture of Training • Meritocracy in the Profession of Arms • Security Cooperation in Support of Theater Strategy • Seizing the Initiative by Establishing the Rule of Law During Combat Operations • Army Doctrine Publication 3-0: An Opportunity to Meet the Challenges of the Future 8 “America’ Army – Our Profession” • Education for Critical Thinking • Narcissism and Toxic Leaders • Discerning the Role of the Narrative in Strategy Development • Center for Army Leadership Response to “Empirically Based Leadership”



Defence for and from Pakistan • Roketsan – One of the Major Players in the Global Defence Market • Pakistan’s Defence Policy in a Tough Neighbourhood • Mission System for Maritime Patrol Aircraft • Enhanced Border and Perimeter Security • Armour • “The Opportunity

to Build a Durable Architecture for Peace in Or Region” • Strategic Partnerships: The Future of Pakistan’s Defence Industry Growth • NBC Threat and Equipment • Equipping the Front-Line Responder • Non-Lethal Weapons and Technologies Resources and Techniques and Lessons Learned • The Future of Non-Lethal Weapons and Technologies • Non-Lethal Industry Review • Defence for and from Indonesia • Lightweight Vehicles for and in Indonesia

ÖMZ (Österreichische Militärische Zeitschrift), Germany, no. 5, September-October 2012

Deployment of Armed Forces Applying the Population-Centred “Comprehensive Approach” • Defensive Revengism • The Growing Influence of the Military Islam and al-Qaeda in Africa • Austrian Security and Defence Policy under an Altered General Set Up an Opportunity to Sharpen the Profile

of the Austrian Armed Forces • Necessity and Limits of Supranational Migration Management according to the Case Study Southern Italy • “B-Gendarmerie: A Successful Experiment Compared with BGS and KVP”. End and Triple Fresh Start • Religion and Politics in Authority • General Karl Schrems

ÖMZ (Österreichische Militärische Zeitschrift), Germany, no. 6, November-December 2012

The “Arabian Springtime” Liven Up the West Sahara Conflict • Geostrategy and Cartoscience • Soldiers! The Second Polish War Has Begun! • The Arabian Springtime and its Security-Political Consequences • Cyber Defence – A Military Challenge • “New Wars” – Non-Governmental War Protagonists • Smarter Defence, the Comprehensive Approach, and an Answer to the Question “Why Do We Need NATO?” • The Divided Kurdish Opposition in Syria

ÖMZ (Österreichische Militärische Zeitschrift), Germany, no. 1, January-February 2013

The Strategic Situation at the Turn of the Year • Leadership and Strategy: How to Lead Progressively in Time of Upheaval • The Common Foreign and Defence Policy Is still a Long Way Off Unilateralism and Short Budgets • Conception and Methodical Aspects of Phrasing and Implementing the National Strategy • The German Jihad – Taking Stock • Energy – Autarchy without Nuclear Energy • The Muslim Brothers as an Alternative in the Near East • Volkswehr-Reichswehr-Bundeswehr: The Re-establishment of the Armed Forces in the Loser States of the First World War, the German Empire and (German) Austria – A Comparison (Part 1)

NATO Support Agency Continues Evolution • Alliance to Deploy Cyber Rapid Reaction Team • Technology and the Warfighter Come Together in NATO • Teaming with Industry Major Thrust for NATO • La Collaborazione con l’industria una Spinta Importante



per la NATO • Dutch Navy Sails Into New Era, New Challenges • Universities Develop New-School Biometrics • Plug-and-Play Biometrics • Better Security Is in the Cards • Advancing Afghanistan's Cybersecurity • Information Technology Firm Sees Major Trends Bolstering Sales to Defence, Intelligence • Events Demonstrate Viability of Rapid Acquisition

Signal, USA, vol. 67, no. 3, November 2012

Pacific Command Adjust to New Regional Emphasis • Information Priorities in Asia-Pacific • Building Bridges across the Pacific • The Armada Down Under • Era of Change for Unmanned Systems • Swarming to a Better Robot • Mixing with Manned Aircraft • The Tactical Edge Sees Data Interoperability • Budgetary Pressures no Hindrance to Turkish Military • Turkey's Companies Assume Larger Military Role • Turkish Groups Provide Industry, Government Bridge

Signal, USA, vol. 67, no. 4, December 2012

Being Number Two Will Not Do for Information Dominance • NGEN Bidders Offer Continuity with Change • Navy Lab Bridges the Research Bench and the Fleet • New Ships Sail in the Persian Gulf • Technologies Advance the Art of Antenna Science • Researchers Whip Up Antenna Technology • Antenna Experiments Yield Military Benefits • Multi-Antenna Research Overcomes Frequency Shortage • Laboratory Research Twists Antenna Technology

Signal, USA, vol. 67, no. 5, January 2013

US Government Bets Big on Data • Too Much Information Imperils Big Data • Desperately Seeking Big Data Standards • Reading, Writing and Big Data Basics • Korea Exercise Changes the Game • Senior Government Executives Bridge Burgeoning Gap • NATO Addresses Its Info-Centric Future • Obstacles Loom for Pacific Realignment.

Selection and Translation

Dr Mihai POPESCU, Delia PETRACHE,

Cătălina ROJIȘTEANU

National Military Library



FOR THE ATTENTION OF THOSE INTERESTED IN SUBMITTING ARTICLES TO “RMT”

Manuscripts submitted to the editorial staff should be sent by mail or email, edited in *Microsoft Word*, *Times New Roman*, size 14, justify, and they should have no more than 8 pages. The **graphic illustration** – schemes, figures, tables should be designed using *CorelDraw*, and maps and images – in *JPEG* format.

Manuscripts should be written in accordance with the academic standards and adopting the norms in the Longman Dictionary of Contemporary English, available at www.ldoceonline.com. Abbreviations and acronyms should be either avoided or explained.

To optimise our collaboration, submissions should be accompanied by the following: name, phone/fax number, email, address of the institution and other relevant information.

RMT Editorial Staff reserves the right to make editorial changes regarding the style, grammar and length of the manuscripts. Authors will be consulted, in case the changes could affect the form or the content of the manuscript.

We expect You, with interest and hope, to submit your articles for publication, mentioning that manuscripts and relating materials are not given back to authors. Thank you for your understanding!

The Editorial Staff

The editorial and layout process
was completed on 12 April 2013.



Cover 1: The opening session of the meetings of the NATO Military Committee in Chiefs of Defence Session, NATO, Brussels, 16-17 January 2013. Photo: www.nato.int

Cover 3: Ambassador Kolinda Grabar, NATO Assistant Secretary General for Public Diplomacy, addresses staff gathered for the opening of the exhibit "Celebrating Female Leadership within the International Staff at NATO", 8 March 2013, Brussels, Belgium. Photo: www.nato.int

Cover 4: The statue of Prince Alexandru Ioan Cuza on the Romanian Patriarchate Hill. Photo: Valentin CIOBÎRCĂ at www.mapn.ro



<http://www.mapn.ro/smg/gmr>