JOURNAL OF DEFENSE RESOURCES MANAGEMENT

No. 2(2) / 2011

BRASOV - ROMANIA

Şerban LUNGU

Director of Defence Integrated Planning Directorate

Romanian Ministry of National Defence

CURRENT NATO AND EU INITIATIVES IN THE DEFENCE PLANNING FIELD - IMPLICATIONS FOR ROMANIA -

In the field of defence planning, NATO and EU membership, involves, inter alia, a multitude of initiatives in which Romania should participate or take action. Broadly, this article addresses four important initiatives, namely the transition to the New NATO Defence Planning Process, the Multinational Innovative Approaches, the Lisbon Critical Capabilities Commitment and Pooling & Sharing. These initiatives aim at facilitating the accomplishment of the tasks set out in the relevant NATO and EU planning documents.

On 2 April 2009 NATO authorities approved the Outline Model for a NATO Defence Planning Process (NDPP) aiming at a more coherent and comprehensive approach to defence planning. The new model was later complemented by an Implementation and Transition Plan which provided the practical arrangements for the transitional cycle of the new process.

The new concept and the associated mechanism were endorsed by Defence Ministers in their June 2009 meeting. The NDPP represents a step change in NATO's ability to assist nations in the efforts to develop their forces and capabilities. It also has the potential to engage military and non-military aspects in a more cohesive manner, avoiding duplication of efforts. The new NDPP stemmed from the necessity to provide the Alliance the capabilities needed to meet its Level of Ambition, and, on short term, addresses the shortfalls identified by means of the lessons learned from the past and current operations.

Romania fully supports the implementation of the new Defence Planning Process, which is more transparent, more integrated, coherent and effective. In this respect, we had to harmonize the national defence planning system with the NDPP. One of the challenges was the transition from a six year to a ten year period, due to obvious reasons. Another challenge was raised by the development of procedures to deal with capability development in the broadest meaning (the former issue has been dealt with, while the latter is expected to be implemented by 2012). Therefore, a couple of defence planning or planning related bills are expecting approval, namely The Defence Law and The Defence Planning Law. Both are taking into account the provisions and recommendations of the new NATO Defence Planning Process and provide the bedrock for a capability-based defence planning process. Procedures have been developed and improved since 2010, starting with the five step approach of NATO 2008 Force Goals (FG) implementation [1].

Without going to great lengths, it should be mentioned that is was a comprehensive review, emphasising jointness, involving a working group established for this purpose, with representatives from all Major programs, and almost all central organisations within the Ministry of National Defence (MoND). One very significant gain of the exercise was the development of a strong linkage between procurement planning (and, more widely, capability development) and infrastructure planning, a goal which has not been quite achieved before. Several innovative and extremely cost-effective solutions have been identified to provide stopgaps before major procurement programs are initiated by building on ongoing programs, on existing, but strangely ignored, capability elements (some of them of Romanian design and/or make), and on creativity. All multinational programs with Romanian participation, as well the capabilities developed through NATO Security Investment Programme and Foreign Military Sales were fully accounted for, unlike before. It came

as a little surprise that in specific situations FG requirements were already met, while in others anticipated delays were eliminated or condensed. This exercise and its outcome were deemed as quite effective and useful during the assessment of Romania's national plans by NATO Staffs and Strategic Commands representatives in September 2010 in Bucharest and recognized by the Allies in April 2011 in the Defence Policy and Planning Committee.

The impact of the financial crisis and the ensuing fiscal consolidation on the development and fielding of forces and capabilities is profound for the near term. Quite a few NATO states experience difficulties in improving their contribution to operations, in meeting their current commitments or in pursuing the requisite transformation of their forces. The reduction in available resources increases the importance of Allies working together to secure the capabilities needed for Alliance operations. Multinational cooperation, whether in small groups or large, encourages and contributes to enhanced interoperability and burden sharing.

Notwithstanding the inherent challenges, multinational approaches can help address critical shortfalls and enable NATO to meet the tasks set out in its new Strategic Concept. Due to the global economic crisis and the lack of financial resources, these might be an option for most nations to develop the capabilities committed to NATO. They shall also play a key role in getting greater return on investment in the use of defence expenditure and in securing, in a collective manner, capabilities that are obviously beyond the reach of the utmost majority of individual nations. In some cases, national requirements are too small to be cost-effectively pursued by the nation concerned alone, but through cooperation with others, a project can achieve critical mass. The Alliance has a long history of multinational cooperation, with a view to equipment acquisition, operation and maintenance/support (whether of pre-existing or and joint development/procurement of new equipment) and the cooperative preparation and organisation of forces (education, training, joint and combined forces, multinational headquarters and so forth).

The proposals resulted from the Lisbon Summit tasking on multinational approaches and other innovative ways of capability development should, of course, contribute to supplying the Alliance with the necessary forces and capabilities. They should be developed in a way that complements and is consistent with the new NATO Defence Planning Process.

Subsequently, a special working group was created at Allied Command for Transformation (ACT) level in order to identify the possible domains of

cooperation. Out of the proposals package submitted by the ACT Task Force on Multinational and Innovative Solutions to nations, more than half (29 out of the current total of 46) were identified as of interest for Romania. We do believe they represent a very useful means to eliminate critical capability shortfalls, including those related to Alliance Operations and Missions. Romania is highly encouraged by the work already done by the ACT and expects all nations to join. The work done by the ACT Working Group on this matter proves that we are on the right track and encourages us to focus on strengthening cooperation in this process.

The current Strategic Concept, approved by the Heads of States and Government HoS/G in 2010 at the Lisbon NATO Summit, includes a clear statement of defence priorities and it is accompanied by an agreed set of essential new or improved capabilities and reforms, which is referred to as the Lisbon Package or the Lisbon Critical Capabilities Commitment.

To reach this end state, the Alliance should both embrace reform and, while acknowledging that national defence budgets are tight, pledge that NATO's most critical capability requirements receive the highest funding priority and the firm backing of Allies. Therefore, NATO's Secretary General has been tasked to implement the following two strong initiatives in support of the new Strategic Concept:

1. a bold and comprehensive initiative to reform how NATO does business, from how it undertakes military operations to the way it manages resources. In this respect, a major reform package was agreed at Lisbon and addresses: command structure improvements, committee reductions, agency consolidations, Headquarters organization and operating procedures;
2. an initiative to implement a shortlist of ten critical capabilities - a Lisbon Critical Capabilities Commitment - that is:
    - affordable within realistic budget projections for nations and NATO;
    - comprised of NATO-sponsored or NATO multinational capability-oriented programs, with the objective of better using resources in order to improve the usability and effectiveness of Allied forces, and where possible, to promote partnerships with other countries and institutions, especially with the EU.

Romania is strongly committed to finding pragmatic possibilities and ways to participate into the Allied effort of providing NATO's most needed

capability requirements, both on short term, through the elimination of current operational shortfalls, and on medium and long term through the generation of capabilities able to deal with the new challenges envisaged by the new Strategic Concept. Our participation to significant NATO subsidiary organizations providing capabilities to the Alliance (NAPMO, NAMO, and NAGSMO [2]) stands proof to this. It is worth mentioning that we joined these organisations before multinationality gained prominence at NATO level, acknowledging their full value.

The European Union corresponding initiative is pooling and sharing. This concept represents the focal point of current European defence policy in the field of capability development and the only feasible and real answer that can be provided to current shortfalls. As no European country can maintain the full spectrum of military capabilities (the trend is rather strongly in the opposite direction), they are increasingly on bilateral and multilateral initiatives. Romania is already involved in the Combat Equipment for Dismounted Soldier, C-IED Theatre Exploitation Laboratory and the European Air Transport Fleet projects. Recently, 20 projects were identified as of interest for Romania under the "pooling and sharing" initiative. They were selected after a review aimed at achieving synergy and avoiding duplication with the similar endeavour undertaken by ACT.

To conclude, Romania remains committed to the process of developing capabilities required by NATO and EU in order to perform their full spectrum of missions. In this respect, we fully support any multinational approach or innovative solution targeted at improving the capability development process, within the framework of the NATO Defence Planning Process and consistent with our commitments to NATO and EU.

ENDNOTES

[1] (i) Revalidation of national implementation plans against the FG requirements. In case of discrepancies, plans were adapted in order to focus on the specific FG requirements (and not on overly optimistic add-ons, with little, if any, connection with the financial reality). Due to financial limitations implementation it is aiming only to NATO assigned units for the planning period;

(ii) Identification of possible material alternative solutions for FG implementation where the case;
(iii) Reassigning the FG implementation responsibility to another armed service or central organization, aiming at cost effectiveness, where possible;
(iv) Identification of other implementation solutions; requesting implementation deadline postponement not excluded as a last resort;
(v) Report to national authorities and assessment/review with NATO authorities of the FG implementation status and perspective/deadlines.

[2] NATO Airborne Early Warning and Control Programme Management Organisation, responsible for all aspects of the management and implementation of the NATO AEW&C Programme (the capability consists of 17 E 3A aircraft, UK providing an additional seven E 3D), established in 1978, is the oldest such initiative and has a long and proud record in NATO operations. NATO Airlift Management Organisation, which supports the operations of the Heavy Airlift Group (three C 17 III Globemaster), is the most creative and efficient (costs are shared by the participants in accordance with committed flying hours, not macroeconomic figures), includes 2 PfP nations; it delivered an usable capability very fast, being established in 2008. NATO AGS Management Organisation will plan, control, manage, supervise and implement the Allied Ground Surveillance Programme, hence providing a significant capability enhancement in the field of Intelligence, Surveillance and Reconnaissance. It is worth noting that NAPMO comprises only 17 of the Allies (soon 16), NAMO ten, while NAGSMO 14 (soon 13). Similar national capabilities notwithstanding, this leaves quite a lot of room for burden sharing.

CONTENTS

COLLABORATIVE MULTI-LEVEL PLAN MONITORING

Mohamad K. ALLOUCHE*, Jean BERGER**

*Defence Scientist, C2 Decision Support Systems Section, Defence Research & Development Canada - Valcartier, Quebec, Canada
** Defence Scientist, Defence Research & Development Canada - Valcartier, Quebec, Canada

The recent worldwide connectivity and the net-centricity of military operations (coalition-based operations) are witnessing an increasing need for the monitoring of plan execution for enhanced resource management and decision making. Monitoring of ongoing operations is the process of continuous observation recording and reporting. In this process the plan becomes a resource that needs to be managed efficiently. The centralized approach to plan monitoring soon reaches its limits when plan execution is distributed across different organizations/countries. We propose a new framework that would allow different monitoring nodes distributed across the network. An efficient propagation mechanism that allows information exchange between the different nodes would also be needed. The main purpose of this mechanism is to present the right information, to the right person, at the right time. To cope with a rapid increase of information flow through the network, an efficient alarm management mechanism allows the presentation of the information with an appropriate level of details.

Key words: *Plan Monitoring, Execution Management, Alarm Management, Resource Management, Multi-Agent Systems, Distributed Monitoring.*

1. INTRODUCTION

The growing connectivity in information framework is constantly challenging the Canadian National Defence to cope with the complexity of operations and to respond to the increasing demand for rapid information sharing capability. The execution of operations is no exception, a great deal of Canadian operations involve different organizations and/or different countries (coalition operations). In this context, an efficient management of resources is a key element for the success for any distributed and decentralized operation. The decentralization of operations makes it even more difficult to monitor their execution. The information is often transmitted through legacy systems that lack integration and synchronization and cause lack of critical information which impact the whole decision making process during the conduct of missions. Monitoring ongoing

mission requires considering the mission plan as a specific resource that needs to be managed efficiently.

In order to cope with the increasing demand of networked and collaborative planning and execution of operations, it is important to have multiple representations of the same plan at different levels of details. This allows easy access to any information at the right level of detail based on the user profile, need, and perspective.

2. RELATED WORK

Monitoring, in a broad sense, is a process involving state information gathering specifications and actions, property verification/ validation and execution tasks aimed at detecting unsuitable system condition occurrences by controlling and triggering specific alerts or countermeasures whenever necessary. By and large, monitoring tasks may be generally centralized or distributed, information-bounded (*e.g.* cultural, operational/political, privacy, security or competitive constraints purposes), resource-bounded (*e.g.* sensory, computational and communication and related cost), and comprises a variety of characteristics defining property verification, information-sharing protocols, analysis, forecasting and planning (*e.g.* value of monitoring, focus of attention coordination and state variables selection, actions to control or mitigate alert avalanches-tree-based incremental aggregation, window (time-interval)-based state monitoring, pull/push-based polling, false-positive and redundant alerts handling, sampling rates, reporting or response pre-conditions).

Despite a diversity of nomenclatures reported in the literature, some convergence on commonly known concepts can nonetheless be determined. In this respect, a relevant taxonomy which provides users with the ability to understand and perform relevant comparison task with respect to the state-of-the-art in monitoring approaches and techniques is presented in [1]. The specification language branch of the taxonomy classifies the language that is used to define monitored properties, the abstraction level of the specification, and the expressiveness (property type and the level of monitoring) of the language. The latter can be based on algebra, automata, or logic.

Single or multiple monitoring objectives refer to certain properties of significance such as safety, liveness, security oriented and performance related properties. Safety properties [2] are expressing undesirable conditions to occur. These may involve some invariants, a temporal sequence of valid predicates, properties that check values of variables, or properties dealing with resource allocation.

Other temporal categories include properties such as progress and bounded liveness, as well as timing properties. In terms of platform, monitors can be differentiated as software and hardware monitors [3].

Monitoring approaches are usually time-based and event-based. Time-based monitoring involves time point (*e.g.* threshold monitoring [4] or time interval (*e.g.* value monitoring [5] state variable sampling and checking for threshold violations, whereas event-based monitoring relies on dynamic behaviour through analysis of a sequence of events (*e.g.* tracing [6]). However, time-based value monitoring can sometimes solve specific issues related to event-based threshold monitoring [7] by using an alert triggering commonly referred as "Threshold Crossing Alert" (TCA). This represents an important aspect in the context of interactive execution monitoring [8]. The dependency context is also elaborated in [9] while reactivity and its real-time related aspects are discussed in [10]. Issues related to interactive alerting during plan execution represent a vital and challenging topic in relation to the response and adaptive changes in the course of action. In this respect, monitoring technologies have been used in continuous planning frameworks such as those described in [11]. In this area, relevant research efforts are dealing with agent systems as presented in [12]. In other respect, alerts may be classified in categories [13] such as detection, operational constraint violation, suggestions or adversarial activities.

Distributed monitoring tasks aim at revealing accurate condition verification in multi-player settings. This research area supports the use of game theory and mechanism design. In addition, the "theories of collaboration" involve directing agents in conjunction with the monitoring of the execution, by modeling elements of team collaboration along with levels of partial knowledge.

3. PLANS AND PLANNING

In our framework, plans are considered as the main resources to be monitored during plan execution. It is then important to describe the different types of existing plans and the different planning processes that build them.

A Campaign Plan is a sequence of planned, resourced and executed military operations designed to achieve strategic and operational objectives within a given time and area. A campaign plan would be monitored by insuring that decision points on different lines of operations are met.

An Operations Plan (OPLAN) is by definition the Main Plan to which all supporting plans will refer to. Some examples of OPLAN are:

Attack Plan, Defensive Plan, or Counter-Movements Plan.

A Support Plan supports an OPLAN usually in terms of resources. The resource will be available for a predefined period of time at a given location. The availability of a resource does not imply the consumption of this resource. Depending on the evolution of the supported plan these resources could be used or not. Some examples of supporting plans are: Mobility-Counter Mobility Plan, Fire Plan, Air Support Plan, etc.

A Contingency Plan is designed for contingencies, has been wargamed and can be reasonably anticipated in an area of operations. The commander's reserve could be part of such a plan.

The Enemy Plan is used during the wargaming sessions during which intelligence Staff will proof many Enemy COAs in order to better prepare our own troops for an operation.

The types of plans discussed above must not be confused with the types of planning. Planning is the process followed by the Staff to design and build a plan. Depending on different constraints, there are different types of planning processes:

• The Deliberate Planning is usually chosen in the absence of time constraints or threats. It consists in elaborating and adopting plans in view of a known situation or incident.

• The Crisis Planning consists in the elaboration and adoption of plans in order to face an existing crisis or an expected one. The first three stages of the Operational Planning Process (OPP) are often shortened in crisis planning.

• The Forces Planning is usually done in stage two of the OPP in order to evaluate our own Forces and the opposing ones.

• The Multinational Planning or Joint Planning is usually performed by a Joint Operation Planning Group (JOPG), which is normally formed for a coalition or inter-army operations.

4. PLAN MONITONRING CONCEPT (PMC)

This section describes a conceptual representation of the different plan abstract levels. **Figure 1** depicts the multi-relations between a plan and the multiple abstract levels. The information axis is composed of four (4) dimensions. Therefore, each task has information in each dimension. Each layer is oriented to present the information with a specific view or a specific concern. The graph in the cube represents one plan (one instance of a plan) in the dimension of plans. This plan is spread all over the other four (4) dimensions. This conceptual model is intended to present the right information at the right level of detail for the right person, in such manner that an operator does not have the

impression of information overload but only the necessary information needed to perform a task.

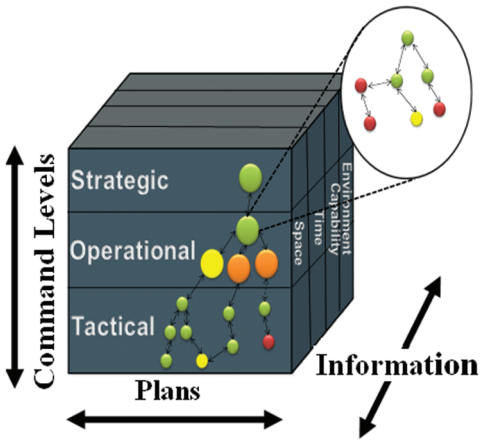

Fig. 1 *Plan Monitoring Concept (PMC)*

4.1. COMMAND LEVELS

The first dimension covers the traditional levels of Command. A plan is usually associated with a level of Command.

At the Strategic Level a nation, often as a member of a group of nations, determines national or multinational (alliance or coalition) strategic security objectives and guidance, develops and uses national resources to achieve these objectives. This level has a temporal horizon of more than 1 year.

At the Operational Level, the headquarters determine objectives and provide resources for tactical operations. The operational level links employing tactical forces to achieving the strategic end state. The Operational Level defines the objectives to achieve the desired final state of the Strategic Level. This level has a temporal horizon of 1 to 12 months.

At the tactical level, the commanders use combat power to accomplish missions. This level has a horizon of days.

4.2. PLANS AND RESOURCES

The second dimension covers all available plans and resources to be managed or monitored at the different levels of Command. The top level (*e.g.* Strategic) gives a macro representation of a plan (orientation or desired effects), which will be more detailed according to the current perspective, as we move down through the Operational and the Tactical levels.

4.3. INFORMATION

The third dimension covers all types of information required to cope with the current military context. This dimension has four (4) general categories: Space, Time, Capability and Environment, which encompass all relevant information that contributes to answering the following questions: who is doing what, where, when, why and how?

The Time dimension covers the synchronization aspects of an object such as the beginning and end times of a task for instance. Time is a

measure of a continuum expressed in terms of hours, minutes and seconds in a precise manner. Time dimension value can be real, relative to an action or scheduled for a future action. For example, a task can be started only if the enemy reaches a particular position in the field.

The Space dimension covers the spatial characteristics of an object (geo-referencing objects).

The Capability dimension gives all relevant information about the state of an object such as specification, consumable rate and availability.

The Environment dimension gives all external information that may have an impact on an object such as terrain or weather conditions or the enemy presence in the field.

With this approach, an operator can navigate (zoom in or zoom out) and have the right level of detail for the required information. The four aforementioned categories can be used to model the commander's intent at any level of Command.

5. MONITORING FUNCTIONS AND APPLICATION

Curiously, the military doctrine is not very clear about plan monitoring and frequently refers to the "Operation Planning Execution Art". In our framework, we use the S.M.A.R.T. model used by the United Nations (UN) to qualify a good monitoring function. This model checks if the information is Specific, Measurable, Attainable, Relevant and Time-based.

An important aspect of the monitoring functions is to be able not only to measure any deviation or change within the object itself but also to be able to detect or even better, to measure the impact of the change on the other objects of interest.

To illustrate the application of our Plan Monitoring Concept (PMC), we use an Army generic scenario often referred to during captain training: "A Canadian Mechanized Brigade Group is part of a coalition in a NATO lead operation in a friendly fictitious country in order to push back an enemy invasion". The details of this scenario go beyond the scope of this paper. **Figure 2** presents the different elements of the operational plan that was developed in order to reach the high-level goal of pushing back the invader. It is important to notice that there are four views for the plan corresponding to the four dimensions of the PMC: Time, Space, Capability and Environment. Furthermore, in each of the views, each presented element has four hooks (T, S, C, E) that allow to link this element to other elements according to the four dimensions. For instance, in Figure 2, an Enemy Air Drop would have a direct impact on the Canalize task, which is linked by its Environment hook. The Time view will then allow the user to see what

delays are caused by this event (Gantt chart part of Figure 2). The Space view (the part with the smaller map view of Figure 2) allows the user to visualize the possible maneuvers of the enemy after the air drop (dashed red lines on the central smaller map). These maneuvers are usually analyzed during the wargaming phase performed during the operational planning process.

Finally, the Capability view would allow the user to have an idea about the current state of the resources (view at the bottom of Figure 2).

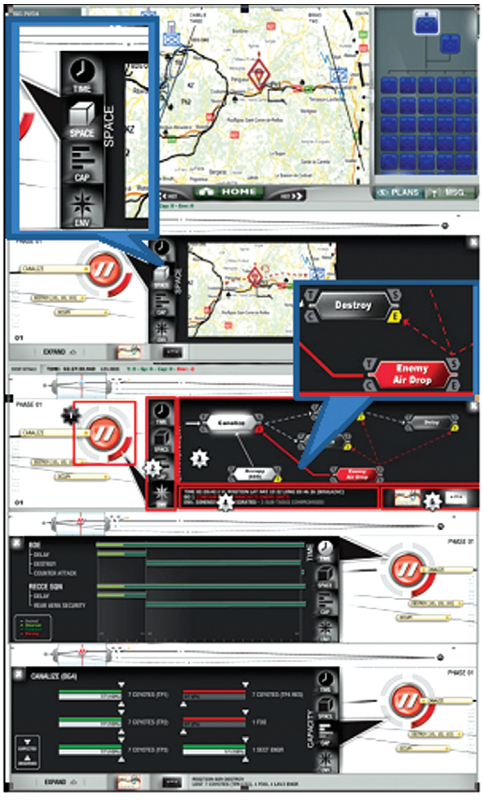

Fig. 2 *Application of the monitoring functions*

In this case, two of the resources (red lines) were severely affected by the enemy air drop. The Commander needs then to choose among the available courses of actions available in the plan by taking into account the current state of the resources.

6. CONCLUSIONS & PERSPECTIVES

In this paper, we address the execution monitoring of plans. According to Moltke's theory of war, "*no plan survives contact with the enemy*". Consequently, the decision-maker needs to be aware of the performance and progress of current plans and their related resources. The proposed Plan Monitoring Concept draws automatic links between plan elements, allowing the Commander to be aware of any change and also the impact of a change on other plan elements. By doing so, the information will be filtered and only the right level of detail will be presented to the Commander. It is also important to mention that the framework allows different analyses based on the perspective of the user. We are currently investigating the use of multiple representations of plan elements in order to collaboratively monitor the execution of plan at different levels of abstraction. In this context, different players (in a coalition for instance) with different perspectives may join the monitoring

task. The information needs to be presented at the right level of detail for each player. For this reason, it is important to have different representations of the plan elements to reflect those levels of detail. In future work, we will investigate the use of influence graphs to represent more complex interrelations between the different plans elements.

REFERENCES

[1] N. Delgado, A. Q. Gates, S. Roach. *A taxonomy and catalog of runtime software-fault monitoring tools*. IEEE Transactions on Software Engineering, 30(12):859-872, December 2004.

[2] Koen Claessen. *Safety property verification of cyclic synchronous circuits*. Electron. Notes Theor. Comput. Sci., 88:55-69, October 2004.

[3] Dennis K. Peters, David Lorge Parnas. *Requirements-based monitors for real-time systems*. IEEE Trans. Softw. Eng., 28:146-158, February 2002.

[4] Graham Cormode, S. Muthukrishnan, and Ke Yi. *Algorithms for distributed functional monitoring. In Proceedings of the nineteenth annual ACM-SIAM symposium on Discrete algorithms*, SODA '08, pages 1076-1085, Philadelphia, PA, USA, 2008. Society for Industrial and Applied Mathematics.

[5] Ling Huang, Minos Garofalakis, Anthony D. Joseph, and Nina Taft. *Approximate decision making in large-scale distributed systems*. NIPS Workshop: Statistical Learning Techniques for Solving Systems Problems (MLSys). Vancouver, B.C, December 2007.

[6] Mohamed Ziad Albari. *A taxonomy of runtime software Monitoring systems*. http://www.informatik.unikiel.de/~wg/Lehre/Seminar-SS05/Mohamed_Ziad_Albari/vortrag.pdf, 2005.

[7] Graham Cormode, S. Muthukrishnan, Ke Yi. *Algorithms for distributed functional monitoring*. In Proceedings of the nineteenth annual ACM-SIAM symposium on Discrete algorithms, SODA '08, pages 1076-1085, Philadelphia, PA, USA, 2008. Society for Industrial and Applied Mathematics.

[8] David E. Wilkins, Thomas J. Lee, Pauline Berry. I*nteractive execution monitoring of agent teams*. Journal of Artificial Intelligence Research, 18:217-261, 2003.

[9] Barbara J. Grosz , Sarit Kraus. *The evolution of sharedplans*. In Foundations and Theories of Rational Agency, pages 227-262. Kluwer Academic Publishers, 1998.

[10] Abdel-Illah Mouaddib, Shlomo Zilberstein. Knowledge-based anytime computation. In Proceedings of the 14th international joint conference on Artificial intelligence - Volume 1, 775-781, San Francisco, CA, USA, 1995. Morgan Kaufmann Publishers Inc.

[11] Karen L. Myers. CPEF: *A continuous planning and execution framework*. AI Magazine, 20(4):63-69, 1999; David E. Wilkins, Karen L. Myers, John D. Lowrance, Leonard P. Wesley. Planning and reacting in uncertain and dynamic environments. Journal of Experimental and Theoretical AI, 7(1):197-227, 1995.

[12] Karen L. Myers, David N. Morley. *Human directability of agents*. In Proceedings of the 1st international conference on Knowledge capture, K-CAP '01, pages 108-115, New York, NY, USA, 2001. ACM.

[13] David E. Wilkins, Thomas J. Lee, and Pauline Berry. *Interactive execution monitoring of agent teams*. Journal of Artificial Intelligence Research, 18:217-261, 2003.

CBRN TERRORISM: A CONTRIBUTION TO THE ANALYSIS OF RISKS

Dušan VIČAR*, Radim VIČAR**

*Tomas Bata University, Department of Crisis Management and Logistics, Crisis Management Institute, Uherské Hradiště, Czech Republic
** University of Defence, Faculty of Economics and Management, Brno, Czech Republic

The World Trade Centre attack of September 2001 and the subsequent anthrax letters brought the need for Chemical, Biological, Radiological and Nuclear (CBRN) counter-terrorism preparadness into focus. By and large, our understanding of the nature of CBRN terrorism derives entirely from military the paradigm of chemical and biological warfare. An examination of recent CBRN terrorism events such as the 1995 Sarin attack on the Tokyo subway system by a terrorist cult and the 2001 anthrax letter attacks in the United States of America show that the military paradigm of CBW defence cannot be applied to CBRN terrorism.

Key words: *Chemical, Biological, Radiological and Nuclear Terrorism, CBRN agents, CBRN terrorism, CBRN Counter-Terrorism.*

1. INTRODUCTION

Terrorism is a socially dangerous phenomenon both at the national and international level. It is a deliberate, preconceived use of force or threat of force, usually often focused on not involved persons to trigger a fear, through which terrorists' political, ideological and religious requirements are to be met. In a global war, everyone is a target of terrorists, especially unprotected civilians, as they are the easiest target. Definitions of terrorism have certain common elements emphasizing the systematic use of physical violence directed against civilians to cause a general climate of fear when innocent people are targeted for political and social change. There are no commonly accepted definitions of CBRN materials, threats or incidents. For the purpose of this paper, however, it is most useful to use a rather broad description of the terrorist threat concerning CBRN materials: all uses of chemical, biological, radiological or nuclear substances and materials for terrorist purposes.

An increasing interest of terrorists in chemical and biological warfare agents, an easy access to technical information, technologies, materials and specialist data and an increase of terrorist attacks with the use of chemical and biological weapons highlight the fact that the risk of this kind of terrorism is

growing. Chemical and biological agents attract terrorists because their production is easy and can be easily acquired. Even a small amount of these agents, due to their toxicity and contagiousness, can result in heavy losses of unprotected population. Of course, terrorism does not use only such chemical and biological agents, which are designed for special military purposes. Just realize a great amount of tanks transporting industrial toxic agents on roads and by railway, which may easily become a focus of terrorist action.

An exact number of casualties or losses of lives because of CBRN assets usage cannot be estimated, but experts agree that the greatest effect of their use will be a large-scale wave of fear and panic. Awareness of public and readiness of special units of the so-called first responders (*i.e.* fire-fighters, police personnel, emergency medical and rescue service) to a CBRN terrorist attack can prevent an uncontrolled spreading of fear and panic and, consequently, will impede terrorists to attain their main objective- to scare and dismay their victims.

2. HISTORICAL EXAMPLES OF THE USE OF CBRN DEVICES IN TERRORIST ATTACKS

On 20 March 1995 in Tokyo subway, a sarin, chemical agent, was used for a terrorist attack against non-protected civilians. A religious cult Aum Shinrikyo acquired information and technical means to plan, produce and use chemical agents for its own terrorist goal. This attack was a first example of a large-scale terrorist attack with the use of toxic chemical agents that was considered by that time to be a domain of military forces.

The impact of this terrorist attack was measured in terms of numbers of casualties and injured, gaps in the technical capabilities of first responders and a clear demonstration of the use of CBRN assets to attain the targets of terrorists. The sarin attack affected 5,100 persons, out of which 12 were casualties, 40 heavily affected, more than 900 moderately affected and many slightly injured. About 300 members of the rescue teams, including fire fighters, policemen and emergency medical personnel were also injured. These secondary victims were caused by insufficient knowledge, training and technical capabilities to cope with a threat posed by the use of chemical weapons. It also revealed the fact that those who want to rescue must be properly protected.

This sarin attack also showed how important were the means to handle with immediate consequences of threat, such as, for example, protective equipment for rescue teams, detection and diagnosis equipment, means for hasty decontamination of victims, rescue teams and buildings, and how important a proper coordination and communication of individual

first responders against this type of terrorist attack was.

In October 2001 in the U.S. a series of anthrax attacks occurred. The first information of affected persons came from Florida. Other cases of anthrax inhalation and skin infection appeared in New York, New Jersey, Maryland, Virginia, Pennsylvania and Connecticut. Letters containing powder anthrax were sent to various mass media and state administration authorities. In total, there were 22 affected persons, 11 of them with symptoms on their skin and 11 more with respiratory system problems. Due to the inhalation of the agent, 5 people died.

This case shows another example of the use of CBRN assets for terrorist attacks. Same as in Tokyo, terrorists acquired necessary information and equipment needed to launch an attack using the biological warfare agent. The so-called anthrax letters showed that use of combat biological agents could have new intended or not intended aftermaths that were not sufficiently evident in connection with the use of chemical and biological agents to date. The impact on the civilians was terrible (32,000 persons had to undergo a basic antimicrobiological treatment, out of them more than 10,000 persons due to a suspicion of being contaminated by this anthrax were recommended to undergo another 60-days treatment). Another effect of anthrax letters was a great contamination of buildings and infrastructure. Some post office personnel were contaminated and several died. If we take into consideration a characteristic of the terrorist attack already mentioned in the second example (*i.e.* the letters were carefully stuck down and an explanatory message was attached) it is improbable that the post office personnel were also an objective of terrorists. The consequences of these anthrax attacks were solved months and years after this event, as opposed to an immediate emergency in case of attack by chemical warfare agent.

These attacks showed a need to quickly detect the attack, identify its character and, given the nature of the attack, to also diagnose the persons contaminated by anthrax, which posed an enormous burden on the health care system. It was also necessary to find the contaminated persons and to provide them a timely and proper care. While great efforts were made to remove the attack consequences, the specialized laboratories processed more than 120,000 tests for B. anthracis, 69% of which were carried out by the laboratories of the public medical facilities. For preventive and curative care, 3.75 million antidotes were needed. This called attention to the need to improve readiness and immediate response, which had not been so urgent in the case of previous terrorist attacks.

3. CBRN TERRORISM ATTACKS EXPERIENCE

With the attack against the World Business Center in September 2001 and following letters containing anthrax, security and the need to be prepared to counter chemical, biological, nuclear and radiological

attack became the focus of attention of strategic planning and national security of almost all countries. Since then they have been considered as one of the most important challenges to the democratic civilization. From a general viewpoint, a present understanding of the substance of terrorism that uses chemical, biological, nuclear and radiological assets issues especially from a military paradigm of the conduct of chemical and biological warfare. These paradigms include tasks of intelligence service, lists of potential threatening by CBRN assets, assessment of potential targets of attack, risk analysis and conception of defense as a deterrent means. However, from an analysis of terrorist attacks with the use of CBRN assets it results that against terrorism, which uses the CBRN assets, a conception of defense against chemical and biological warfare in an armed conflict cannot be applied.

To attain a better readiness for defense against terrorist CBRN attacks, as well as development of prevention and response methods, it is necessary to create new models of better response to such attacks. A present approach to countering this type of terrorism resembles the approach to a military threat, namely the use of the intelligence service to identify the capabilities of an enemy, to have proper knowledge of NBC weapons threat designed by an enemy for combat purposes, analysis of related risks and weapons that can be applied, and also the assumption that a well prepared defense will discourage an enemy from an attack. The question is if these assumptions are valid.

Terrorism, especially CBRN terrorism, calls for new approaches to intelligence information. It requires collecting, analyzing and exchanging information not only on the organizations, but also on the individuals that work independently. There are very little events reviewed in such a great detail as the attacks of 11 September 2001 in New York and Washington and attacks by anthrax-laden letter. The intelligence services, especially, were criticized because they did not provide timely warning so that preventive action could be taken. Taking into account many indications that terrorists hired new members, trained them, planned and organized attacks, as well as the duration of the preparations to counter these, as mentioned by the media, the activity of the intelligence services can be perceived as a failure. However, it is necessary to admit that from the actions of individuals who pursue wider terrorist goals, it is not simple to acquire "*information*" needed for an effective countering of a terrorist attack.

The military science, due to the transition from conventional weapons to the new non-conventional conduct of combat, started to use the term of "*asymmetric war*". Terrorism is sometimes considered a civilian analogy to asymmetric war, where small-scale non-conventional attacks have a great impact. On the other

hand, other sources view this analogy as imprecise because the target of the attack is not the armed forces, but unprotected civilians.

4. LEGAL INSTRUMENTS AND CBRN TERRORISM

Terrorist attacks have highlighted the need for further efforts of the entire international community in combating this threat. In the fight against global terrorist networks national or regional response is insufficient. Global cooperation thus becomes a matter of vital importance. For example, the European Union is a key player alongside with the United States of America (USA), China and Russia, on the international scene and has a decisive influence on the security situation in the world. By its nature, it is a supranational organization, the body of international relations that, after the adoption of the Lisbon Treaty, has a legal personality. The threat of a terrorist group acquiring CBRN materials has led governments and international organisations to adopt far-reaching regulations and programmes to defend populations against the associated risks.

A common European approach to security issues of the contemporary world was outlined in December 2003 when the EU Council met in Brussels and adopted the final version of the European Security Strategy (ESS). For the first time principles were established and clear objectives for the enforcement of security interests of the EU based on core values and identified a range of threats and challenges to security concerns set. The main threats classified in the ESS are: terrorism, proliferation of weapons of mass destruction, regional conflicts, state failure and organized crime.

These threats were described as new, more diverse, less visible and less predictable. On the other hand, the traditional military threat in the form of large-scale aggression against any Member State of the EU seems unlikely. The ESS considers an attack using CBRN weapons as one of the biggest threats to the security of the EU, especially thanks to advances in biological sciences which may increase the potency of biological weapons. The most frightening scenario is terrorist groups gaining CBRN weapons. In such a scenario a small group could cause damage similar to what was previously possible only for states and armed forces.

Tackling terrorist access to CBRN material is currently considered a priority for the European Union. This is acknowledged by the European Union Counter-Terrorism Strategy adopted by the Council on 1 December 2005, and by the *"EU Strategy against proliferation of weapons of mass destruction and their means of delivery (WMD)"* adopted by the European Council on 12 December 2003.

The EU counter-terrorism strategy fights against terrorism on four main objectives: prevent, protect, pursue

and respond and with wide range of measures (co-operation in fields ranging from intelligence sharing to law enforcement and the control of financial assets in order to make it easier to find, detain and bring to justice terror suspects).

The overall goal of CBRN policy is to reduce the threat and damage from CBRN incidents to the citizens of the European Union, by way of a coherent, prioritised EU CBRN Action Plan. The EU CBRN Action Plan is not a legal instrument. The Action Plan foresees three main areas of CBRN security work: Prevention (*i.e.* ensuring that unauthorised access to CBRN materials of concern is as difficult as possible); Detection (having the capability to detect CBRN materials in order to prevent or respond to CBRN incidents); Preparedness and response (*i.e.* being able to efficiently respond to incidents involving CBRN materials and recover from them as quickly as possible).

Protecting the population from terrorism and other criminal threats is a high priority for the EU. As exemplified by events around the world, there is continuous interest of terrorists in acquiring CBRN materials. The Member States are primarily responsible for many of the areas of work which are covered by the current policy package. They are responsible for protecting their citizens from CBRN threats by a host of different measures, and with the involvement of a wide range of responsible authorities.

5. A DEFENCE AGAINST CBRN TERRORISM

In defence against chemical and biological agents and in technical preparations, agents known to have been developed and used by an enemy as a weapon have always been highlighted. Such agents are on the list that serves as a basis for the development of protective technical means and capabilities, including presence detection, identification, protection, medical measures and elimination of effects of these agents. The above-mentioned emphasis on known chemical and biological warfare agents, even bias towards these agents, led the military to conceived the defence against such an attack as a defence against a "specific threat". Thus, defence against terrorism, in a way, can be viewed as defence against a "non specific threat". A spectrum of CBRN means of attack provides terrorists with a nearly unlimited amount of toxic, hazardous and infectious agents, the production, stocktaking, tactical or strategic use of which are not included by military into a traditional analysis of risks. That is why, in coping with terrorist attack, civilian first responders must apply an integrating approach, which takes into an account all types of threat.

Based on the intelligence information and analysis of threats and risks, in order to minimize impacts of CBRN attack, militaries must invest into the defense and protective equipment. They perform training to ensure a minimum impact

on the armed force's operational capabilities in case of eventual CBRN attack. Also, a proper assessment of the technologies and the new possibilities to support chemical and biological defense on the basis of prediction of potential threat in the next 10-15 years is used. The result of this assessment is identification of areas where knowledge should be amended, as well as recommendations on how to achieve it submitted. A part of this assessment is also a presumption that these technologies, if used, will serve as a deterrent. Certainly, this consideration assumes that enemy's behavior is rational or that enemy is able to analyze strategic or tactic employment of chemical weapons and take decisions based on the level of defense and capabilities of the opponent.

However, this assumption does not apply to terrorism. Traditional deterrent means that it cannot stop a group of dissenters without any concrete objective. Terrorism that uses the CBRN assets has the greatest deterrent and destructive effect because its target is unprotected civilian inhabitants. There are not such measures that could protect civilian inhabitants under all circumstances. Even the strictest security and preventive countermeasures cannot prevent suicide assassins. There will always be vulnerable groups of people. A targeted protection, for example, of significant buildings, cities or various events can make terrorists change their plans and attack other, less protected groups of people.

A critical issue is the training of the first reaction forces for CBRN attack. Before the personnel in the first line can say what action must be taken and what equipment they need to eliminate the aftermaths of such attack, they must understand the basic aspects of chemical, biological and radiological agents. Though an average rescuer does not need to be a chemistry expert for these agents, nor must he know how to treat every approximately 300 human pathogens, he must anyway know symptoms of effects of these agents and basic treatment and decontamination procedures. Having this information, he is able to transform his knowledge and experience and apply them in a case of terrorist attack.

In the case of threat from potential hazardous agents the rescue technical teams use standard procedures which encompass basic target functions like site inspection for threats, hazardous agent identification, risk and threat analysis, assessment of protective equipment necessity, information and rescue resources co-ordination, hazardous agent control by preventing its spreading, decontaminating the area and consolidating the overall situation. After a terrorist attack, other important functions must be added: people's evacuation, casualties' clearance and treatment and evidence material gathering.

6. CONCLUSIONS

The CBRN terrorism counter-measures, in contrast to the recommendation of the armed forces structures, require shifting from a

decision-taking process based on the detailed analysis of the enemy capabilities to an approach based on the risk analysis. To establish priorities, many countries carried out extensive consultations resulting in risk analyses of the CBRN assets. Conclusions of such analyses are used by intelligence services, anti-terrorist units, scientific agencies and institutions and rescue teams that have to cope with actual events.

However, a detailed research of the potential use of CBRN assets for terrorism does not guarantee that an actual CBRN attack can be avoided. Risks related to the use of CBRN assets and materials show how important it is to have consolidated capabilities available to respond to the threat and properly train rescue teams for a partnership within a scientific-technological community. Knowledge on CBRN assets that ensue from the usual military practice of preparedness must be carefully reviewed and immediately quit if they do not meet the for civilian protection requirements in case of threat. It seems to be vitally important for the EU Member States to ensure: legislation (which determines the duties and responsibilities of citizens in the constitution and other laws in accordance with EU strategic and legal principles), the systematic training of experts in the field of crisis management, performance and intelligence cooperation at bilateral and multilateral international levels, scientific research and technological cooperation, the systematic preparation of specialists (special forces) to combat terrorism, population information and preparation, a functional integrated rescue system, finance and logistics.

REFERENCES

[1] Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union.

[2] Countering Terrorism. Final Report - Part I (2003), RTO/SAS-049 Specialist Team. Brussels.

[3] Evropská bezpečnostní strategie [online]. Council of the EU, [cit. 2011-5-10]. http://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf.

[4] Jenkins, Brian. *International Terrorism: The Other World War.* In Charles W. Kegley, Jr. (ed.), (2003) The New Global Terrorism: Characteristics, Causes, and Controls. Upper Saddle River, NJ: Prentice Hall, ISBN 978-0130494139.

[5] Kournikakis, B., et al., (2001) *Risk Assessment of Anthrax Threat Letters.* DRES Technical Report 2001-048, Defence R&D Canada.

[6] Laqueur, Walter. Postmodern Terrorism. In Kegley, Jr. (ed.), (2003) The New Global Terrorism: Characteristics, Causes, and Controls. Prentice Hall, NJ Upper Saddle River, ISBN 978-0130494139.

[7] Proceedings of Lecture Series on Chemical and Biological Defence (2005), Brusel, RTO NATO.

[8] *RTO Combating Terrorism.* Workshop Report. USA, Arlington, 2002.

[9] Svoboda, I., *et al.*, (2010) Politický extremismus a terorismus jako ohrožení vnitřní bezpečnosti státu. Univerzita obrany, Brno, p.144, ISBN 80-7418-046-0.

ORIENTATION: THE KEY TO THE OODA LOOP

Dr. Donald A. MACCUISH

Associate Professor, Strategy and Leadership Air Command and Staff College Maxwell AFB, AL 36112, USA

John Boyd's research began by his quest for understanding why Americans flying an inferior airplane in Korea had a higher kill ratio than the adversary. He completed it with his much discussed and written about OODA Loop. What I find quite interesting is that almost everyone agrees that the most important part of the Loop is "Orientation". I heartedly agree. If Orientation is the most important element, for lack of a better word, why do we suggest that the first step is to observe? Orientation drives observation and not the other way around. I will focus my discussion on this portion of the OODA Loop. I conclude the discussion by linking Col. Boyd's cycle to leadership and organizational structure.

Key words: *decision-making, observation, orientation, decision, action*

1. INTRODUCTION

I rather enjoyed reading the last issue of the Journal of Defense Resources Management. Two articles really caught my attention. I thought Dr. Gherman's "*The Second Revolution in Military Affairs*" was both interesting and informative because he used Colonel John Boyd's OODA Loop as a basis for his discussion concerning information processing [1]. Although I enjoyed reading the article and thought he made several good points I slightly disagree with him on two counts. In his abstract he suggested that action is associated with movement and firepower. He emphasized this point again in the second paragraph of section 2 on page 58. Although in the military context that is often the case, action does not necessarily mean physical movement nor does it always have to be kinetic in nature. Although "*Orientation*" involves information processing it is much more dynamic than he suggests; so much so that computer programs can be a useful tool, but a human must still use his or her faculties to determine the appropriate action to take or not to take.

The other article I enjoyed was "*Effective Strategic Decision Making*" by Dr. Vasilescu [2]. One of the margin notes I made in my copy of the Journal was that an individual does not necessarily have all the information deemed necessary to make a quality decision regardless of context. This is a dilemma faced by decision makers whether they are in the military, government, business or elsewhere. Sometimes you just have to make a decision, observe what happens, and take appropriate action to improve the situation as quickly as you can - the OODA Loop.

The second point I found interesting was the notion he brought up in the first paragraph of section 2 on page 102 about rationality. What is rationality? Rationality has a cultural component that we cannot dismiss. If we are not aware of the other person's cultural heritage we might misinterpret our observation of the situation.

Periodically, I have to remind myself of this reality. To do so I use the analogy of a person suffering from a mental disorder, schizophrenia for example. When a schizophrenic makes a decision, it may be quite irrational to me or from most peoples' perspective, but to him or her it is quite rational.

My positive reaction to these two articles inspired me to write about John Boyd's OODA Loop with a focus on Orientation. I have been studying the OODA Loop for several years and would like to share some of my insights. I think we often look at the OODA Loop much too simply. I have sat through too many lectures at ACSC and read too many articles in which the OODA Loop is illustrated by a diagram similar to the one in **Figure 1**. There is a problem with this depiction. By thinking of the OODA Loop in this manner, one can easily conclude that it is a progression through stages. Such is not the case. One does not observe then orient then decide then act, and then go through the process again. The OODA Loop cycle is much more dynamic than that.

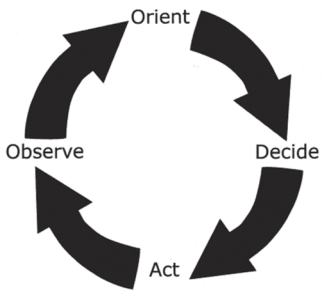

Fig. 1 *Common misrepresentation of the OODA Loop*

Because of this fact we cannot develop a computer model to replicate it, but computer systems can help the decision maker in several ways. To my knowledge, Col. Boyd diagrammed the OODA Loop process once[3]. He drew it in 1995 as part of a five-slide PowerPoint presentation. **Figure 2** below is Colonel Boyd's depiction of his OODA Loop. Pay particular attention to the text box below his depiction of the OODA Loop. This is very important and proves at least from Col. Boyd's perspective the diagram at Figure 1 is not the OODA Loop.

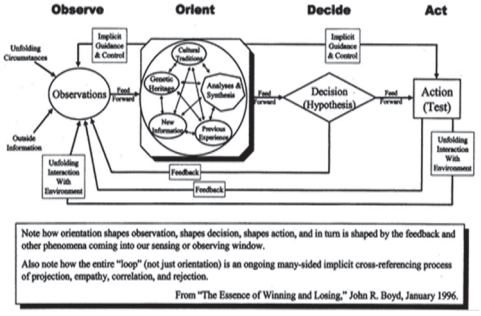

Fig. 2 *Boyd Cycle/OODA LOOP*

I think the first sentence in the text box of Figure 2 is critical to our understanding of the Boyd Cycle. Notice that Boyd states that

*"...**orientation** shapes decision, shapes action, and, in turn, is shaped by the feedback and other phenomena coming into out sensing or observation window."* [4] What he is saying is that if you are not oriented correctly then what and how you observe the situation will be distorted. And, no matter how quickly you go through your OODA Loop cycle, your resulting decision will necessarily be flawed.

He also notes that the "loop" is quite dynamic. It is an ongoing many-sided implicit, not explicit, cross-referencing process of projection, empathy, correlation, and rejection process. We continually react to environmental stimuli not essentials are filtered out. If we are not properly oriented then our attention is directed to and we process the stimuli as we expect and not as it really is.

My question then becomes if you are not properly oriented to your situation does it make any difference how fast you go through the Loop? I contend that you will probably make an incorrect decision and thus select an inappropriate course of action. The result will be you have just gotten inside your own OODA Loop. For example, President Bush and his advisors believed Saddam Hussein had weapons of mass destruction. Because of this orientation all the information they received was processed in this light. In hindsight we know that their orientation was incorrect and decisions were made with devastating consequences. Richards, in his briefing *Why Did We Lose in Iraq*, captures this quite well by quoting General Michael Hayden *"We just took too much for granted. We didn't challenge our basic assumptions."* [5]

2. DISCUSSION OF ORIENTATION

Orientation, noted Boyd, *"represents images, views, or impressions of the world shaped by genetic heritage, cultural tradition, previous experiences, and unfolding circumstances"* [6]. Later in his briefing he states: *"Orientation is the schwerpunkt. It shapes the way we interact with the environment-hence orientation shapes the way we observe, the way we decide, the way we act. In this sense orientation shapes the character of present observation-orientation-decision-action loops-while these present loops shape the character of future orientation"*. [7] Corum notes that what Boyd is saying is *"that a relationship exists between an observer and what is being observed"* [8]. This relationship is governed by cognitive interactions of genetic heritage, cultural tradition, previous experiences, and the unfolding experiences taking place. These interactions within the orientation loop(s) are continuous and dynamic. They are all functions of the brain, the thinking process, thus not really measurable. As a result, the value of intuition cannot be understated.

Boyd held that Orientation is the schwerpunkt of the cycle. By this he meant that orientation provides focus

and direction for one's efforts [9]. I do not know why Boyd placed *"genetic heritage"* first. To be honest, I am not sure that it matters. People who have discussed Boyd say little about genetic heritage and what he meant by it. I have several ideas about its significance in this process.

In an article for Delta Sky Magazine Anderson and Molloy equated a person's genes to the body's instruction manual [10]. Nobel Laureate Herman Joseph Muller said that genes are "*the fundamental unit of heredity*" as well as the *"basis of life"* [11]. David Cummings of the City of Hope Medical Center notes that genetics account for a number of common disorders such as heart disease, diabetes, and mental disorders such as depression [12]. McElheny adds hypertension, coronary disease, and rheumatoid arthritis among others to the list [13]. Thus people can have a predisposition to disease, illness, and addictiveness thanks to our genetic heritage.

Each of the mentioned genetic possibilities can, and sometimes do, have an effect on how people orient themselves and interpret the events they observe. With that said, Keller reminds us that *"genes do not act all the time, but instead need to be turned on and off in response to specific stimuli"* [14]. I suggest that the environment is the switch that turns them on and off? Ambiguity immediately comes to mind as does a high stress environment, such as combat or in the business world the pressure to meet a sales goal. Further, Montagu states that neither heredity nor environment alone makes us what we are. *"Genes interact with other genes and with the environments in which they occur. The environment interacts with the genes and the genes interact with one another."* [15]

But that is not the only way genetics affects the way we orient to our environment. Personality is another factor. Kroeger and Thuesen write that according to Jungian theory people are born with a predisposition for personality preferences [16]. In 1990 Voges and Braund wrote personality is influenced by both heredity and the environment with heredity being more influential than either upbringing or social pressure [17]. Although the influence of one's early years can be mitigated for better or worse later in life it is most difficult to overcome those early influences. One's personality and behavior undoubtedly have an impact on orientation. This impact may not be a crucial initially, but as new information is forthcoming and the pressures of the situation become greater reorienting to these new elements can have a significant impact on people, especially those in leadership positions.

The influence of cultural traditions is also an important factor with regard to orientation. We Americans believe we are exceptional. We do not need cultural traditions. They are for everyone else. After all, we Americans have something else. We have our notion of individualism, democratic institutions, etc. Thus, all too

frequently we see others less favorably and this arrogance has gotten us into trouble on more than once occasion.

Another cultural factor often missed is the culture of one's work environment which can offset some genetic heritage factors. For example, why does the American automaker General Motors find it so difficult to compete with Toyota, Nissan, or Hyundai in the marketplace? Each military service has its own culture as well and in combat situations differences in service culture profoundly influences the orientation of service leaders [18].

I ask the reader to reflect on what I have written with regard to cultural traditions in the broad sense here to his or her own. Consider, for example, your cultural influences based on your religious persuasion, ethnicity, nation and/or region, etc. How do these aspects of culture effect how you make observations and decisions? What type of action or actions would you take because of these cultural influences in any given situation?

Genetic Heritage and Cultural Traditions are not the only factors that influence our orientation. Previous experiences are also factors. Previous experiences range far and wide from childhood to the present. What constitutes previous experience? In the military setting previous experiences would primarily come from time spent in similar or somewhat similar situations. And if we have not been in a similar situation then one we have been told about or studied. The same would be true in a business setting. But previous experience includes more than physical experience. It also includes the cognitive images we develop from education, reading, study, etc. There is no doubt that previous experience is quite important to us. It provides a base of reference, but it can also hinder us. Interestingly we often see what we want or expect to see and this often does have negative consequences in how we process new information. The best example I can think of at the moment is recorded in Gordon and Trainor's book Cobra II which is about Operation Iraqi Freedom. As American forces were moving northward they were increasingly attacked by Saddam's Fedayeen. Soldiers and Marines at battalion level and below readily recognized the threat and adapted, but those higher up the chain of command ignored the reports from their subordinates. It was not until General Wallace gave an interview stating *"The enemy we are fighting,... is a bit different than the one we war-gamed against, because they are paramilitary forces."*[19] Accurately processing new information is vital, but it must be done with an open mind.

The last element in Boyd's Orientation cycle has to do with analysis and synthesis. The two are not the same. To get his point across Boyd, in his *The Strategic Game of ? and ?*, provided the following illustration. He asked the audience to imagine that they are on a ski slope with other skiers, in an outboard motor boat, riding a bicycle, and your son is looking at a toy tank with rubber treads all at the same

time [20]. Then, he asked them to break the various images into smaller parts (analysis). In the seventh slide he asked them to retain only these images - the skis off the ski slope, outboard motor off the boat, handle bars off the bicycle, and the rubber treats off the toy tank. He then asked his audience to pull those items together and what did they have. His answer was a snowmobile (synthesis).

Most good decision makers are quite good at analysis. Being able to synthesize information at one's disposal is quite a different matter altogether. This is an important skill for each of us to master, and an extremely important one for senior commanders, government officials, and people in business. Boyd held that each of these elements were quite dynamic and not only affected how we orient to the situation before us, but also influence the decisions we make and the actions we take. He also believed that synthesis was the basis of creativity [21].

3. LEADERSHIP AND ORGANIZATIONAL STRUCTURE

There are two things that govern the speed and accuracy of the OODA Loop Cycle. These are leadership and organizational culture. Richards in his 2005 *Certain to Win* briefing noted: *"Ultimately, a culture or climate that encourages people to use their initiative to further the goals* of the organization" [22] is what determines OODA Loop speed. Both are dependent upon leadership. Increasing OODA Loop accuracy and speed requires that leaders at every level trust those below them in the hierarchy. Trust is built over time.

Boyd used the German term *auftragstaktik* to express the relationship and trust that must exist between leaders and their subordinates. Quite simply he was saying that everyone needs to focus on the goal or objective. The subordinate is then given wide latitude to accomplish the goal. This requires that leaders issue implicit instructions (mission type orders) and not explicit direction. This does not mean that there are instances in which explicit direction is required, but that should be the exception and not the rule. The strategic bombing campaign of Germany during WWII is an example on a situation requiring explicit orders, centralized command and control, and decentralized execution. Had it not been this way, the effort would have been less effective.

During the early days of WWII the German Paratroopers who attacked the impregnable Eben Emael Fortress had this latitude. Eighty-six men in 11 gliders took off from German bases on 10 May 1940. In route the tow rope of the glider carrying the commander of the operation parted and the aircraft was forced to land. Second glider was released early and did not take part in the operation either. Thus, only 67 made it to their objective, yet these few men were able to neutralize the fortress with 30 minutes of landing. They were aided in their effort because the defenders were operating under a centralized command and control system.

Van Creveld provides us with a more interesting example in his book Command in War. In his discussion of mobile warfare he discusses both the 1967 and 1973 Arab-Israeli Wars. In 1967 the Israeli Army was operating under the model I have advocated here. The Israeli General Gavish stated that *"there is no alternative to looking into a subordinate's eyes, listening to his tone of voice"* [23] to get a true sense of what was actually going on. The net result was that commanders at all levels, most importantly General Gavish, were well oriented and were able to flow through their OODA Loop Cycles faster than their adversaries. But that is not the instructional piece I wish to convey. The very battalion and brigade commanders who were responsible for winning the 1967 war were the senior leaders during the disastrous 1973 war. In those six years they instituted a centralized command and control, and decentralized execution system. The Israeli Defense Force was transformed from a military force that was quite agile to one that was much slower.

Leadership is critical. Leadership determines organizational culture and command climate. Both of which effect orientation and thus OODA Loop speed.

4. CONCLUSIONS

In conclusion, what is the OODA Loop, or Boyd Cycle? It is a model developed to explain a natural phenomenon of how human beings process information, think, and make decisions. It is however much more. The OODA Loop also illustrates how people and organizations learn and therefore how they adapt or fail to adapt to their surroundings. Each of us goes through the OODA Loop cycle without realizing we are doing it.

I am rapidly going through OODA Loop cycles as I think about the best way to end this essay for I want it to be a piece that encourages readers to reflect on what others have written in this and past issues of the Journal. I want them to become more aware of what it is and where we need to develop greater understanding. Further, I encourage the read to become more reflective in hopes of improving their OODA Loop cycle.

Finally, Dr. Gherman is correct: it is an information processing system provided one is oriented correctly. Dr. Vasilescu is also correct for it depicts how we make decisions, but unless we are oriented correctly, decisions will be fraught with error. It is a model showing how we learn and adapt or fail to adapt to our ever changing environment. And I believe it is a model for leadership also.

REFERENCES

[1] Gherman, Laurian (2011). *"The Second Revolution in Military Affairs"* in Journal of Defense Resources Management. Brasov, Romania: Military Technical Publishing Center.

[2] Vasilescu, Cezar (2011). *"Effective Strategic Decision Making"* in Journal of Defense Resources Management. Brasov, Romania: Military Technical Publishing Center.

[3] Boyd, John R. (1996). The Essence of Winning and Losing, slide 3. http://pogoarchives.org/m/dni/john_boyd_compendium/essence_of_winning_losing.pdf; See also: http://www.projectwhitehorse.com/pdfs/boyd/The%20Essence%20of%20Winning%20and%20Losing.pdf
[4] ibid. at http://pogoarchives.org/m/dni/john_boyd_compendium/essence_of_winning_losing.pdf.
[5] Richards, Chet (2006). *Why Did We Lose in Iraq?*, Slide 2.
[6] Boyd, John (1987). Organic Design for Command and Control, (briefing), slide 13.
[7] ibid., slide 16.
[8] Coram, Robert (2002). *Boyd the Fighter Pilot Who Changed the Art of War.* Boston: Little, Brown and Company. p. 323.
[9] Richards, Chester (2005). *Certain to Win John Boyd's Strategy for the 21st Century Or, anywhere other the first is a tie for last.* Slide 54.
[10] Anderson, Mark and P. Molly (August 2010). "*Your DNA, Decoded*", in Delta Sky Magazine. p. 73.
[11] Keller, Evelyn Fox (2000). *The Century of the Gene.* Cambridge, MA: Harvard University Press. p. 3.
[12] McElheny, Victor K. (2010). *Drawing the Map of Life Inside the Human Genome Project.* New York: Basic Books. p. 56.
[13] ibid., p.214.
[14] Keller, p. 79.
[15] Montagu, Ashley (1959). *Human Heredity.* Cleveland: The World Publishing Company. pp.70 and 71.
[16] Kroeger, Otto and J.M. Thuesen (1988). *Type Talk the 16 Personality Types that Determine How We Live, Love, and Work.* New York: Tilden Press. p. 13.
[17] Voges, Ken and R. Braund (1990). *Understanding How Others Misunderstand You.* Chicago: Moody Press. pp. 27 and 28.
[18] See Builder, Carl H. (1989). *The Masks of War American Military Styles in Strategy and Analysis.* Baltimore: The Johns Hopkins University Press for a lengthy discussion on this topic.
[19] Gordon, Michael R. and B.E. Trainor (2006). *Cobra II the Inside Story of the Invasion and Occupation of Iraq.* New York: Pantheon Books. p. 311.
[20] Boyd, John R. (1987). *The Strategic Game of ? and ?*. (briefing), slide 6.
[21] Coram, p. 325.
[22] Richards, Chester (2005). *Certain to Win John Boyd's Strategy for the 21st Century Or, anywhere other the first is a tie for last.* Slide 50.
[23] Van Creveld, Martin (1985). *Command in War.* Cambridge, MA: Harvard University Press. p. 199.
[24] Boyd, John R. (1996). *The Essence of Winning and Losing*, edited by Chet Richards and Chuck Spinney, produced and designed by Ginger Richards (2010), Kettle Creek Corporation, Atlanta, GA.
[25] Griffith, Samuel B. (trans) (1971). *Sun Tzu The Art of War.* London: Oxford University Press.
[26] Hammond, Grant T. (2001). *The Mind of War John Boyd and American Security.* Washington: Smithsonian Institution Press.
[27] Kroeger, Otto and J.M. Thuesen (1992). *Type Talk at Work.* New York: Tilden Press.
[28] Moyer, Mark (2009). A Question of Command Counterinsurgency from the Civil War to Iraq. New Haven, CT: Yale University Press.
[29] Osinga, Frans (2005). *Science Strategy and War the Strategic Theory of John Boyd.* Delft, The Netherlands: Eburon Academic Publishers.
[30] Richards, Chester W. (2001). *A Swift, Elusive Sword What if Sun Tzu and John Boyd Did a National Defense Review?* Washington: Center for Defense Information.
[31] Sawyer, Ralph D. (trans.) (1994). *Sun Tzu The Art of War.* New York: Barnes & Noble Books.

PROSECUTING SOMALIA PIRATES AS TERRORISTS

ODHIAMBO E.O.S.* , ONKWARE K.*, KASSILLY J.*, NTABO O. M.**

*Centre for Disaster Management & Humanitarian Assistance (CDMHA)
Masinde Muliro University of Science Technology, Kenya
**Dept. of Criminology and Social Work, Masinde Muliro University of Science Technology, Kenya

This article starts from the assumption that piracy resembles terrorism in many aspects and attempts to support it through both a theoretical investigation and practical examples. The argument it makes is that Somali pirates should be prosecuted as terrorists. Moreover, it emphasizes the idea that for Somalia's neighboring countries and not only the implementation of such an approach consists in resorting to the antiterrorist conventions already in place. Thus, for example, Kenya Navy as a piracy-fighting agency should rely on these conventions to justify the capture and prosecution of pirates in Kenyan courts. In this respect, we emphasize the idea that only by resorting to an established international legal framework can Kenya identify the tools to counter pirates' actions within legal limits. Moreover, this should be paralleled by efforts towards rebuilding Somalia and its institutions if long-term solutions are to be envisaged in the eradication of piracy in the Indian Ocean. In conclusion, the article looks at the concepts of piracy, terrorism and development in the Horn of Africa, suggests that piracy is a form of Terrorism and, makes a series of recommendations.

Key words: *piracy, terrorism, country development, Kenya Navy, Horn of Africa*

1. INTRODUCTION

Somalia has had no recognised central government since 1991, when President Mohamed Siad Barre was overthrown. Instead, power is divided between various groups including the internationally backed Transitional Federal Institutions and other regional entities such as the breakaway Somaliland, Puntland and Jubaland. International involvement in the country has utterly failed to secure peace. In the past few years, piracy has been on the rise off the coast of Somalia. The International Maritime Community has been hit by ship hi-jackings carried out by Somalia pirates, in the Western Indian Ocean waters off the East Coast of Africa. The Somalia pirates attack and hijack civilian ships carrying cargo through the Gulf of Aden, toward East Africa. The cargo is withheld and the crews are taken hostages until ransoms are paid by either the hostages' home country or the ship owners. The pirates routinely go unpunished; once they release the hostages, they simply return to their speed boats to plan yet another lucrative capture.

United Nations Convention on the Law of the Sea (UNCLOS), article 101 defines piracy as **(a)** any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship or a private aircraft, and directed to *(i)* on the high seas, against another ship or aircraft, or against persons or property on board such ship or aircraft; *(ii)* against a ship, aircraft, persons or property in a place outside the jurisdiction of any State; **(b)** any act of voluntary participation in the operation of a ship or of an aircraft with knowledge of facts making it a pirate ship or aircraft; **(c)** any act of inciting or of intentionally facilitating an act described in (a) or (b) [1].

First descriptions of the practice of piracy are recorded in Homer's The Iliad and The Odyssey, and in Greek mythology. At the time, piracy was considered a reputable profession [2]. It was not until pirates began disrupting vital trade routes to the East and to Africa that cities began to form alliances against pirates [3]. Cicero dubbed pirates "hostis humani generi." [4] Contemporaneous laws drafted by Cicero and the Roman Senate construed piracy as both action against individuals and against the nation as a whole [5]. Pirates were viewed as an enemy of the entire human race and could be prosecuted under municipal law after capture, but the right to prosecute was common to all nations [6].

Terrorism is a component of Peace and Conflict Studies that analyses the interactions between states and other actors in their engagement with each other over legitimacy issues; issues which in turn have a great bearing on development.

Terrorism and development processes have long been considered intertwined. Research shows that acts of terrorism are correlated with economic development and well-being. Persson&Tabellini [7] find empirical evidence consistent with the theory that different political regimes, terrorist or not, have a significant influence on fiscal policy, welfare and corruption. Moreover, Mulligan *et al.* [8] point out that, when economic and demographic variables are taken into account, types of states differ significantly in military spending, torture, execution, censorship, and religious regulation. Thus, the importance and relevance of academic research in the field of piracy, terrorism and development in the Horn of Africa, particularly, is clearly argued [9].

The factors linking piracy to modern-day terrorism and justifying this article's argument that today pirates should be fought just like terrorists are: **(a)** piracy, just like terrorism, embraces the use of terror by non-state actors as a means of coercion directed against states and their citizens; **(b)** piracy has historically been much more than sea-robbery [10]. In this context, piracy, whether perpetrated by private individuals or groups, is to be understood as a political tool

of governments that, by sponsoring such actions, aim to achieve a particular political goal. As such, pirate acts closely resemble terrorist acts; **(c)** pirate motivation throughout history has close resemblance with contemporary terrorist motivation. Similar to the pirates who waged war against a world that they viewed as unjust, today terrorists aim their acts against particular nations, in a war of non-state actors versus states; **(d)** the legal definitions of piracy and terrorism have evolved and have come to resemble one another.

Nowadays, piracy is seen less as sea robbery and more as maritime terrorism, as discussed below and as reflected in modern-day treaties such as the Geneva Convention, UNCLOS, etc. Worth mentioning, in this respect, is the following view: *"As the world has moved beyond the Cold War into a new century and new political realities, so too will piracy law adopt these realities within a new, unabashedly political, definition."*[11] Therefore, it is crucial to understand how piracy, terrorism and development forces interact together in order to make the world a better place via peace. In this paper, we extend the frontier of knowledge in the field of piracy and terrorism by analyzing: **(1)** what is meant by piracy and terrorism; **(2)** the nature of piracy, terrorism and development in the Horn of Africa; **(3)** piracy as a form of terrorism, and **(4)** some recommendations concerning better ways of prosecuting pirates as terrorists.

2. METHODOLOGY

The sensitivity of this study required that primary and secondary researches be employed. Primary data involved interviewing captured pirates in Kenyan jails, former hostages of pirates, as well as selected individuals of Somalia origin found in the North Eastern province of Kenya bordering Somalia.

The investigation method employed consisted in snowballing, where one interviewee led to the other and so on until a sufficient number was reached. Thus, 180 people were interviewed and they expressed their views concerning the nature of piracy, terrorism in Somalia and its threat to Kenya.

Secondary data entailed a critical analysis of the existing literature on the subject under discussion. Consequently, the authors of this paper conducted an extensive library research on papers, reports, journals and books approaching similar topics. The result of their sampling was their division into the following major topics of discussion: piracy, terrorism and development. Thus, some of the findings of this research are presented below.

2.1. PIRACY, TERRORISM AND DEVELOPMENT IN THE HORN OF AFRICA

Dahama and Bhatnagar [12] quoted by MacMichael [13] define community development as the act of bringing forth the potential abilities and qualities of a group's members who live together in a common territory and who have an interdependent relationship with each other. This

definition can be traced back to Carl Taylor. The latter views community development as a method through which people in villages get involved in the improvement of their own economic and social conditions and, hence, become effective in working in national development programs [14]. Thus, as the United Nation argues, community development should be a process by which the efforts of the people themselves are united with those of the government authorities to improve the economic, social and cultural conditions of communities that are part of a nation and to enable them to fully contribute to a national program.

The conclusion to be drawn from the above definitions is the view that community development is more than just economic development. It is a process or effort of building communities on local level with emphasis on building the economy and forging and strengthening social issues [15]. Thus, community development involves moving from the "*traditional*" ways of living to more "*progressive*" ways of living [16]. The central idea here is that for community development to progress well there should be community organization. The nature of community organization will determine the principles by which that community guides itself and, as a result, the extent to which the same community is prone to piracy and terrorism.

Terrorism is, debatably, a humanitarian crisis. The humanitarian and economic costs of conflicts can be astronomical. For this reason, humanity remains engaged in a struggle to prevent conflicts from occurring at the expense of development. This undertaking warrants a better understanding of the reasons underlying conflict emergence and of the means to be employed in preventing or lessening their burdens. A few researchers have discovered that geopolitical factors may affect conflict initiation, payoffs, and outcomes. Filson and Werner [17], for example, develop a formal model of conflict showing that democratic regimes are sensitive to the institutional constraints and costs of war. A careful study of Somalia would explain why there is sustained piracy and terrorism in the Horn of Africa courtesy of the Al Shabab.

2.2. PIRACY AS A FORM OF TERRORISM

Pirates could be more effectively prosecuted if they were treated as terrorists. As a result, a variety of anti-terrorist conventions could become available as basis for their criminal prosecution [18]. Some of these conventions are worth reminding: the Convention for the Suppression of Unlawful Seizure of Aircrafts; the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation; the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf [19]; the Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents; the International Convention against the Taking of Hostages;

the Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation; the International Convention for the Suppression of Terrorist Bombings [20].

These anti-terrorist conventions could either be relied upon directly, should the piracy act fit within the precise framework of one of these acts, or simply be used as jurisdictional and procedural models for the handling of pirates' captures and trials [21].

Piracy, as this article argues, constitutes terrorism on the high seas, and pirates should be treated as terrorists. It is likely that, at present, the activities of Somalia piracy fund Al Shabab terrorist activity. For example, pirate speed boats routinely seize weapons from victim vessels and may be involved in the resale and smuggling of such weapons to terrorist groups.

There are several reasons for which it is very difficult to fight pirates smuggling weapons at state level. Thus, pirate ships routinely fly so-called flags-of-convenience, these ships may be registered through another state's shipping company or the pirates themselves may come from a variety of different countries [22]. Thus, weapon smuggling pirates should be fought at international level, just like terrorists, and should be prosecuted on the basis of anti-terrorist international conventions [23].

Piracy often exists in support of terrorism and serves to fund terrorist groups. There have been situations when pirates have gone after ships carrying valuable cargo; this suggests that pirates may be paying off port and government officials, who supply them with ships' manifests, detailing the ships' cargo, and who then suppress investigations into the captured ships and cargo [24]. Thus, pirates are able to sell the ship's cargo seized for handsome profit, which in turn may fund specific terrorist group.

From a theoretical standpoint, pirates and terrorists differ in one aspect: the latter seem to function on the basis of a particular political or religious ideology, while the former, at least in Somalia, seem purely driven by financial gains [25].

Pirates and terrorists, however, have many similarities. First, both piracy and terrorism are a form of organized crime, with powerful masterminds and numerous executioners. Therefore, going after the latter may not be enough. Instead, one may have to focus on the former. Thus, when going after the Somali pirates, Kenya needs to be able to go after the masterminds that the Somali warlords hide behind the lawlessness of mainland Somalia [26]. Customary international law does not provide capturing nations with the authority to enter Somalia's territory to arrest piracy masterminds and, while some of the 2008 U.N.S.C. resolutions go as far as to authorize capturing nations to enter Somali territorial waters and the Somali land, this option has not been exercised yet by any piracy-fighting nation. However, there are some anti-terrorist conventions that authorize

other nations to enter Somalia in pursuit of pirate/terrorist masterminds and that improve the existing and somewhat limited legal tools already available to nations fighting piracy [27].

Second, both piracy and terrorism exist at a supra-national level, perpetrators of pirate/terrorist crimes act on a private basis, beyond the sponsorship of any particular state, and their targets do not come solely from one particular state. The Somali pirates have gone after ships of many different nationalities so far, and the hostages have come from different countries. Terrorists, similarly, have operated against many different nations like Kenya, for example, and harmed nationals of many different states [28]. Therefore, in fighting pirates, similarly to fighting terrorists, nations should come together to form coalitions, and to rely on international law for tools that will provide them jurisdiction to go after and try captured pirates.

Third, both terrorists and pirates apparently thrive in regions where the reign of the law is little or nonexistent. Thus, while it seems that terrorists have found a safe place in the mountains of Afghanistan, the pirates have been thriving in the war-torn Somalia. Therefore, similar to the means employed to fight terrorism, countries may resort to international law to find authority to conduct air or land-based military initiatives against pirates [29]. Thus, since fighting pirates is not too far from fighting terrorists, Kenya needs to be able to treat pirates just like terrorists. In this respect, it is of utmost importance to widen the range of the already available legal, military and political strategies to attain the aforementioned goal. One such strategy could consist in resorting to anti-terrorist conventions in order to justify for the apprehension of pirates on Somali land or for the prosecution of pirates in Kenya or other regional partners [30].

3. CONCLUSIONS

Modern-day piracy, currently thriving in Somalia and possibly spreading to other regions of the world, is a serious threat to all naval nations, to their ships and crew members, as well as to their cargo. Somalia pirates by the way they conduct their operations (*e.g.* going after prey regardless of its nationality), operate like terrorists. Therefore they can be viewed as a global threat to nations and as menace on all seas. Moreover, they pose an even more serious threat due to their possible association with other terrorist groups, or because their activities could fund such groups.

All countries, and especially those with a significant naval presence, should undertake serious efforts to fight piracy in Somalia, and to ensure that piracy does not re-emerge in another lawless region. Pirates need to be fought in a serious manner: by being captured, prosecuted and punished in the courts of piracy-fighting states. In order to accomplish these goals, piracy-fighting countries should equate piracy with terrorism, should rely on anti-terrorist conventions as a legal basis for the battle against piracy,

and should continue to cooperate in their struggle against pirates. In fact, piracy, exactly like terrorism, thrives in government-less states, war-torn regions, and impoverished areas. Thus, the best long-term solution against piracy may be the developed world's commitment to re-establish functioning order in the developing and failed states, like Somalia.

4. RECOMMENDATIONS

Prosecuting pirates as terrorists is an issue of concern both at national and international level. Therefore, based on the analysis carried out in this article, the authors believe that each state,starting from the correct identification and assessment of its own needs and strategic goals. should fight piracy as terrorism. As a result, as far as Kenya is concerned, a set of recommendations is deemed as of utmost importance to be highlighted at the end of this paper.

A. The greatest threats to the security of Kenyan citizens are diseases and crime. Helping the Kenyan government address these top concerns, especially on the North Eastern and Coast, will make Kenyans more likely to report suspicious activities and might encourage them to more aggressively oppose pirates and terrorist influences. Improving health care and criminal justice may thus do more to combat pirates and terrorism than policies that specifically seek to enhance "counter piracy", "counter terrorism" or "anti-terrorism" capacities [31]. With the massive amounts of counter-piracy and counter-terrorism-related funding provided by the development partners like the U.S. some may argue that Kenyan officials may actually gain from having a continuing piracy and terrorist threat in the country [32]. A possible solution to that could reside in refocussing security assistance to areas, that offer fewer opportunities for patronage than direct payments for military hardware, such as increased governance and disciplined forces training.

B. Stimulating development and foreign aid that helps rural disaffected populations in Somalia and North Eastern, Coastal Kenya will not only earn good will and legitimacy for the Somalia Transitional Government and Kenya central government, but will also increase the price Pirates and terrorists need to pay to buy local assistance and acquiescence. Removing local tolerance of Al Shabab activities and preventing the emergence of safe havens requires persistent development and law enforcement efforts [33]. Somalia Transitional Government, the Kenyan government alongside with their development partners should increase economic development in Somalia and North Eastern Kenya and Coastal provinces. A sustained commitment to improving the economic status of Somalia and North Eastern and Coastal Kenyans is likely to produce two benefits: increased intelligence on piracy and terrorist activities, and increased economic aid which raises the cost of piracy and terrorists of providing social services as a buy-in mechanism for their dangerous goals.

C. One way to reach equilibrium is to focus more on improving the capacityof local business interests to develop their own security infrastructure [34]. Rather than focusing on building a security architecture that secures an unemployed, poor and restless populace prone to radical recruitment, more pragmatic aid policies might support local actors with an economic interest in imposing favorable security conditions. Providing incentives that promote effective, internally generated and sustainable counter piracy, counter terrorism measures tailored to unique local conditions is important particularly to Somalia, North Eastern and Coastal Kenya. North Eastern towns like Mandera and Coastal town like Kiunga in Kenya provide the best opportunity in the country for Al-Shabab and its associated movements to operate. Not as anarchic as Somalia, Northeastern and Coastal Kenya provides a permissive environment for Al-Shabab. Pirates and terrorists operating there may find a sympathetic population from which to draw support.

D. Institutional reforms in the Somalia Transitional Government and Kenya law enforcement sector and economic development on the Somalia and Kenyan North Eastern and Coast are the key to preventing the emergence of pirates and terrorist safe havens. Direct military assistance will have limited impact given the political constraints on the Somalia Transitional and Kenyan government [35]. Instead, counter piracy and counter terrorism efforts should focus on reducing the structural injustices which alongside such factors as weak disciplined forces capacity and disgruntled citizens willing to tolerate the presence of foreign militants may make Somalia and Kenya a valuable operational haven for pirates and terrorists.

E. The problem in Somalia cannot be resolved unless the socio-economic and political issues are addressed.

Kenya Military should therefore act appropriately such as preventive military action [36]. Major maritime powers should enhance partnership with regional countries that are non-partisan on supporting different Somalia clans like Kenya to establish law enforcement and jurisdictional networks, so that pirates are apprehended as often as possible, and so that those who are captured are always prosecuted. The possibility of detained pirates' prosecution should be increased through jurisdictional agreements among maritime powers and regional countries, making at least one criminal forum available for all captured pirates [37]. Shipping companies themselves should contribute to the global fight against piracy, by contributing financially and logistically to maritime countries already engaged in the process of eradicating piracy.

REFERENCES

[1] United Nations (UN), 1982 *United Nations Convention on the Law of the Sea: Provisions relating to piracy.* In: Singapore Shipping Association

Piracy Seminar-(Supplementary Paper 1), 22 October 1999: Singapore Shipping Association, 1999.

[2] Smith George P. Ii (1989) From Cutlass To Cat-O'-Nine Tails: *The Case For International Jurisdiction Of Mutiny On The High Seas*, 10 Mich. J. Int'l L. 277, 191 N. 140; Vivian Louis Forbes (2001) Conflict And *Cooperation In Managing Maritime Space In Semi-Enclosed Sea*, p. 102.

[3] Peppetti Jon D, *Building the Global Maritime Security Network: A Multinational Legal Structure to Combat Transnational Threats,* (55 Naval L. Rev, 2008), pp. 73, 87.

[4] Burgess Jr.,& Douglas R, Hostis Humani Generi: *Piracy, Terrorism and a New International Law*, 13 U. (Miami Int'l & Comp. L. Rev, 2006), pp. 293, 298.

[5] Rubin Alfred.P, *The law of piracy.* 2nd ed. (New York: Transnational Publishers, Inc, 1998), p. 18.

[6] Dubner Barry. H, The law of international sea piracy. Developments in International Law Vol. 2 (The Hague: Martinus Nijhoff Publishers, 1980).

[7] Persson Torsten.,& Guido Tabellini, Political Economics: Explaining Economic Policy, Cambridge: Mit Press, 2000.

[8] Mulligan Cawey B., Ricard Gil & Xavier Sala-I-Martin, "Do Democracies have Different Public Policies than Non democracies?" Journal of Economic Perspectives, 18(1) Winter (2004), pp. 51-74.

[9] Onkware K, Elijah Odhiambo & O.M.Ntabo, Counter terrorism Strategies by Kenya towards Somalia Terrorism. Egerton Journal of Humanities,Social Sciences and Education, Vol. IX, (2010), pp. 99-109.

[10] Bautista M.E.H, Piracy and armed robbery against ships: The Philippines experience. Paper presented at the 32nd Asia-Pacific Economic Cooperation Transportation Working Group Meeting, Singapore, (July 27-30, 2009).

[11] Gibson Helen, *A Plague of Pirates: Modern Buccaneers with Machine Guns Instead of Cutlasses Are Once Again the Scourge of the Oceans* (1997).

[12] Dahama O.P, & Bhatnagar O.P, *Education and Communication for Development.* (Oxford and IBH Publishing Co. Pvt. Ltd, New Delhi, 1987).

[13] McMichael P, Development and social change: A global perspective (3rd ed.), (Thousand Oaks, CA: Pine Forge Press, 2004).

[14] Carl C. Taylor, "Community development program and methods", Community development review, Vo1.3 (December, 1956), p 39.

[15] UNIFEM, A life free of violence is our right. The UN Trust Fund to end violence against women: 10 years of investment, 14-15(2007).

[16] UNICEF, Community-directed interventions for major health problems in Africa: a multi-countrystudy: final report. Geneva, UNICEF/UNDP/World Bank/World Health OrganizationSpecial Programme for Research & Training in Tropical Diseases (2008). (http://www.who.int/tdr/publications/publications/pdf/cdi_report_08.pdf, accessed).

[17] Filson Darren., & Suzanne Werner, "Bargaining and Fighting: The Impact of Regime Type on War Onset, Duration, and Outcomes" with Suzanne Werner, American Journal of Political Science 48:2, April, (2004), pp. 296-313.

[18] Beckman R.C, The 1988 SUA Convention and 2005 SUA protocol: Tools to combat piracy, armed robbery and maritime terrorism. In: Herbert-Burns, R./Bateman, S./ Lehr, P. (Eds)-Lloyd's MIU handbook of maritime security. Boca Raton (Florida, USA: Taylor & Francis, 2009), pp. 187-200.

[19] Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf (London: 8 June 2006).

[20] Cornford Philip & Sarah Crichton, The Ships That Died Of Shame, Sydney Morning Herald, Jan. 14,

At 13, 2003. http://www.smh.com/au/articles/2003/01/13/1041990234408.html.

[21] Beckman R.C, The 1988 SUA Convention and 2005 SUA protocol: Tools to combat piracy, armed robbery and maritime terrorism. In: Herbert-Burns, R./Bateman, S./ Lehr, P. (Eds) – Lloyd's MIU handbook of maritime security. Boca Raton (Florida, USA: Taylor & Francis, 2009), pp. 187-200.

[22] Toby Ecker, "Flags Of Convenience" Raise Security Concerns, (Copley News Service, Feb. 7. 2003).

[23] Chen J, The emerging nexus between piracy and maritime terrorism in Southeast Asia waters: A case study on the Gerakan Aceh Merdeka (GAM). Lehr, P. (Ed.), Violence at sea: Piracy in the age of global terrorism. (Abingdon (Oxon), Routledge, 2007), p. 139-154.

[24] Soulas Delphine, Poverty Stirs Turbulence In Asian Waters; Attacks On Ships Triple Since '93 (Washington Times, Oct. 10, 2003).

[25] Kennedy Elizabeth A, Somali pirates vow to kill American sailors, Apr.15, 2009, http://news.yahoo.com/s/ap/piracy.

[26] Berman John & Aaron Katersky, Pirate Suspect Sobs in Court: 'I Have no Money,' Apr. 21.2009. https://abcnews.go.com/Blotter/story?

[27] Blanco-Bazan A, Legal aspects of piracy and armed robbery against shipping. In: European Commission – Seminar "Piracy and armed robbery against shipping: to prevent, deter, protect and fight against an actual threat". (Brussels, 21 January 2009).

[28] Kiai Maina, Chairman, Kenya National Commission on Human Rights: "The Impact of Counter Terrorism Measures on Human Rights Protection in Africa" presentation in Nairobi at 15th Commonwealth Law Conference on Governance, Globalization and the Commonwealth, (10 September, 2007).

[29] Van Ginkel B & Van Der Putten F.P, The international response to Somali piracy: Challenges and opportunities. eiden: Martinus Nijhoff Publishers, 2010).

[30] Roach J.A, Agora: Piracy prosecutions: Countering piracy off Somalia: International law and international institutions. In: American Journal of International Law, Volume 104, No. 3, July, (2010), pp. 397-436.

[31] McCrummen Stephanie, "Report: U.S. Africa Aid is Increasingly Military," Washington Post, July 18. 2008).www.washingtonpost.com/wpdyn/content/article/2008/07/17/AR2008071702550.html.

[32] Easterly William, The White Man's Burden: Why the West's Efforts to Aid the Rest Have Done So Much ill and So Little Good. (New York: Penguin, 2006).

[33] Atran Scott, "The Moral Logic and Growth of Martyrdom: Instrumental Reasoning vs. Enders, Walter and Todd, "Patterns of Transnational Terrorism, 1970-1999: Alternative Time-Series Estimates". On consequentialist decision making in al-Qa'ida. International Studies Quarterly 46 (2002), pp.145-65.

[34] Felter Joseph, et al., Harmony and Disharmony: Exploiting Al-Qa'ida's Organizational Vulnerabilities (West Point N.Y. United States Military Academy, 2006).

[35] Houreld Katharine, Somali pirates avoid warships to hijack 3 ships, Apr. 6, 2009, available at http://townhall.com/news/world/2009/04/06/Somali_pirates_avoid_warships to_hijack_3_ships.

[36] Duda D & Szubrycht T, The Somali piracy new or old challenge for international community. In: Weintrit, A. (Ed.), Marine navigation and safety of sea transportation, (London: CRC Press, 2009), pp. 743-750.

[37] Geib R, &Petrig A, Piracy and armed robbery at sea: The legal framework for counter-piracy operations in Somalia and the Gulf of Aden. (Oxford, Oxford University Press, 2011).

POLITICAL DEVELOPMENTS IN A GLOBAL WORLD

COL. (ret) Ion GHEORGHE*
LT. GEN (ret) professor, PhD, Marin ILIE **
Lecturer, PhD, Ana Mona ILIE **

* Lawyer, PhD, The Bar of Bucharest, Romania
** "Carol I" National Defense University, Bucharest, Romania

All studies about globalization justly emphasize the unprecedented effects of this phenomenon at national and international level. In this respect ,it is common truth that politics, an essential element in the relationships between states, organizations and other establishments is greatly influenced by this complex process that defines contemporary society. Therefore, the aim of this article is to briefly analyze some of the features of political developments in a globalized world.

Key words: *politics, globalization, evolution, strategy.*

The beginning of the 21st century is under the influence of an increasing complexity and interdependency of human relationships triggered by the irreversible phenomenon coined as globalization. As a result, great changes have occurred in the security field.

Within this framework, many analysts believe that economic growth and state-of-the-art information technology are enough to argue that the world is treading the path of global welfare and political stability. However, there is also a certain degree of carefulness when it comes to making such statements that may prove nothing but illusions. Such reluctance can only be justified by the common truth that the world order asks for consensus. However, unless the existing gap between the more developed, and hence, with more advantages, on one hand and the one at a disadvantage, on the other hand is bridged in such a manner that the latter can foresee the prospect of improving their current lives through their own efforts, it will be difficult to achieve stability and progress. Thus, in the absence of such a prospect for one side of the world, social unrest will continue to emerge within society and between/among states.

It is worth reminding that our world is one of interdependencies and, hence, that triggers consequences for all individuals both at a personal

and general level. In this respect, a researcher in the field of globalization noted:

"At the end of this century, all states join the globalization trend and that leads to interdependent economies. Financial markets weave an invisible web encompassing all countries and, at the same time, deprive of freedom and place constraints on governments. Thus, no state can isolate itself from the rest of the planet." [1]

World leaders and especially industrialized democracies cannot ignore that, in many respect, the gap between the beneficiaries of globalization and the rest of the world is growing deeper and deeper and that can be better observed in the relationships established within society and among states. As a result, globalization is synonymous with growth; growth asks for capital and gaining capital involves getting the highest profits at the smallest costs and, inherently, finding those markets where the profit/risk ratio is a convenient one. Translated into practice, all this means that, one way or another, industrialized countries will absorb a high percentage of the investment capital available at a global level.

Without the right amount of capital, developing countries cannot grow, nor generate employment opportunities for their people. As such, politicians may lose their interest for drawing up and implementing the reforms that are the prerequisite for applying the globalization model. Moreover, for the companies based in these countries it becomes more difficult to access capital from international markets. Therefore, they have to make their capital in their home country and that is possible only by paying installment interests that are higher than in the financial centers abroad. As a result, national companies become less and less competitive, especially in those economic sectors where commercial barriers are emerging.

In the end, when confronted with international competition companies from emerging markets have to choose between going bankrupt or becoming associates of multinational companies. That is exactly the opposite of what supporters of protectionism in industrialized countries foresaw when they warned against the competition of the small salaries paid to the workforce in developing countries. Thus, the long-term solution for these countries trying to enroll on the globalization trend is restructuring.

All of the above facts involve changes in state policies and such changes occur not because of the states' free will but under the pressure of numerous external factors. The latter's goals do not necessarily match those of the states and thus economic, political or tensions appear.

Regardless of the path taken, developed countries will continue to act as engines of globalization. To them, the goal of growth has become an intrinsic one since the ability to make their stocks grow represents their standard of living.

There are two contradictory tendencies in a global world. On one hand, the global market gives the opportunity of becoming extremely rich. On the other hand, it creates new vulnerabilities on the political stage. Moreover, it poses the threat of creating a new gap between a globally digitalized world and those who cannot keep up with it. The impact of these trends on an evolving world is huge. Companies from developing countries are taken over by multinationals. While this process solves the problem of accessing capital, it also increases the vulnerability to domestic political tensions, especially during crises. As a result, within developing countries a political trend directed against globalization emerges.

During the globalization process, a state's economy takes a two-fold path. Some of the domestic companies are integrated into the world economy, most of them under the ownership of international corporations. The rest of the companies remain outside the globalization trend and, thus, pay their workforce the smallest salaries possible, which leads in the end to a bleak social perspective. The national sector depends to a great extent on its ability to control political evolutions in the developing countries. As a result, both types of companies under discussion in this article launch a political challenge. On one hand, the multinationals do not seem to favor key political decisions with a say in public welfare. On the other hand, domestic companies generate political pressures in favor of protectionism and oppose globalization.

The social level mirrors a system of dual dependency. Thus, globalized elites share a set of values and state-of-the-art technologies, while the populations that are outside the global trend are drawn into nationalism, ethnocentrism, liberation movements from what they perceive as the hegemony of globalization and, more often that not, synonymous with the American domination. As a result, anti-globalization movements that all too often resort to violence reflect this gap and are grounded in political reasons.

Therefore, the attacks against globalization could evolve towards a new ideological radicalism, especially in the countries where the leading elite is numerically small, which leads to a deeper gap between the rich and the poor. A new threat looms ahead, especially for the developing countries, and it resides in the emergence of a new category of people at a disadvantage, namely the international category of the poor. That will only make the political consensus needed for ensuring internal stability, international peace and for achieving globalization goals more difficult to achieve.

An open political challenge of the whole process of globalization may not occur too soon, but industrialized countries alongside with multinational companies are widely perceived as its main beneficiaries. However, the clash between the economic reality and the political commitments that

can be made and supported by facts could lead to an earthquake in the worldwide economic and political systems.

Some of the threats mentioned in this article can be avoided by encouraging free commerce. However, even if this may be the solution, the leaders of the world should keep an eye on the political threat. Thus, they should remember the number of years needed by the American political model to become what is nowadays. Therefore, what proved to work in the USA as a result of employing such a model may not as well work in other parts of the world at a more rapid pace than in the aforementioned country. As a result, the measures already in place at a global level do not fully guarantee against a violent outbreak against globalization. It has already been three years since the world crisis began and the essential changes that took place in the political system and policies of many countries are clearer than ever. Austerity measures correlated with other measures resulting in people's rights infringement is what until a decade ago seemed impossible but now is for real. In our opinion, the current crisis is the result of globalization and, hence, the political measures taken to counter it are global by nature, too.

American specialists underline the great extent to which the crisis, that unlike other historical periods when crisis occurred but did not affect the USA (except for the1929-1933 period), had a say in the changes made to the USA's domestic and foreign policy. The great number of those living in poverty, approximately 45 million according to media sources, highlights the impact and seriousness of the current crisis. The forecasts range between moderate optimism and discouraging pessimism. In our opinion, the middle way is better. Therefore, we believe that, even though the crisis' effects will persist for a while, the measures already taken by the UN, USA, EU, G2, G7, G8, G20, by other international organizations, as well as by states will diminish them and, in the end, economic and political stability will be achieved.

No economic system is sustainable without a political one. The challenge for those who believe in globalization is the merger between economic growth and political creativity, as well as achieving a truce between those who view the world from a technical perspective and their critics who argue for a return to an outdated quasi socialist model of control on behalf of the government. The solution is to generate an international feeling of social responsibility without choking successful economic systems with bureaucratic rules and regulations.

Top leaders act under political pressure and are not willing to take a direct approach towards problems that are not obvious from the very beginning and that require long-term solutions that go beyond their mandates. As a result, they are tempted to think, in a conventional manner, that economic phenomena

are autonomous, self adjusting and with no connection with the political process.

According to some remarkable analysts, integration and globalization are two objective processes characteristic of the contemporary world's development. As a result, the fates of nations are deeply interconnected and that lays the ground for mutually advantageous opportunities for them to grow and adapt to the requirements of social and economic progress. However, great historical changes have been the result of humankind's need for a political vision and for a standard of justice.

Within the general framework of globalization, the military field undergoes a series of changes, as well. In this respect, the French professor, Herve Coutau-Bégarie notes:

"We can observe a general tendency towards a globalization of concepts. Such a tendency, in its turn, is the result of the existing interdependencies. Thus, security is no longer a military, but a global one, while UN human security should take into account all types of threats, including the environmental ones or the ones generated by discrimination.

There are a number of theoretical and practical counterarguments to the discussion of strategy as a global concept. Theoretically speaking, the concept of strategy is the object of fields of study that do not share any common thread. There is a political strategy, an economic strategy, an enterprise strategy… Practically speaking and excluding the concept of political globalization, globalization, in general, runs counter the common sense since the tendency is to treat it as an ultimate goal while it is nothing but action". [2]

Moreover, the same authority in the field of strategy says:

"It is necessary to rediscover the essence of strategy. Similar to economy that is characterized by the quest for welfare, to politics in search for the common good, strategy should be based on violent conflict and thus runs the risk of being applied to anything". [3]

We believe it is important to remind that strategy is an instrument of politics. Therefore, the changes in strategy reflect the changes in politics, and all of them take place within the general framework of globalization.

On the other hand, many theoreticians of globalization notice that, as a direct result of the interconnections between the military field and a global world, there is a tendency to adapt the military culture and state policies in the military field to the new developments at international level.

In conclusion, globalization is accompanied by political development that seeks to answer the new challenges of the contemporary world.

REFERENCES

[1] Ramonet, I. (1998) Geopolitica haosului, Doina Publishing House, Bucharest, p.15.

[2] Bégarie, Hervé Coutau. (1999) Traité, de stratégie, Economica Publishing House, Bucharest, p.12.

[3] Bégarie, Hervé Coutau. (2002) Some Notes on Strategy (Breviar de strategie), Sitech, Craiova, p.13.

[4] *** (2000) Millenium Report of the Secretary General, United Nations, Chapter 3, pp.43-44, last retrieved from http://www.un.org/millennium/sg/report/full.htm on 08/22/01.

[5] *** United Nations Charter.

[6] *** - NATO Treaty.

[7] [13] *** NATO Summit - Washington, 3-4 April, 1999.

[8] NATO Summit - Prague, 21-22 November, 2002.

[9] *** NATO Summit - Istanbul, 28-29 June, 2004.

[10] *** NATO Summit - Riga, 28-29 November, 2006.

[11] *** NATO Summit - Bucharest, 2-4 April, 2008.

[12] *** NATO Summit - Strasbourg, France/ Kehl, Germany, 3-4 April, 2009.

[13] *** NATO Summit – Lisbon, 19-20 November, 2010.

[14] *** The National Security Strategy of Romania, 2007.

[15] Claval, Paul. (2000) Geopolitics and geostrategy: political thinking, space and territory in the 20th century (Geopolitica şi geostrategia: gândirea politică, spaţiul şi teritoriul în secolul XX), Corint, Bucharest.

[16] Haynes, Daniel Mark (2000) World Of Risk - Next Generation Strategy For A Volatile Era, John Wiley & Sons Pte Ltd.

[17] Dăianu, Daniel (2001) Why does globalization give rise to such debates? (De ce stârneşte globalizarea atâtea pasiuni?) In "21st Century- Globalization and Identitty" ("Secolul 21 – globalizare şi identitate"), No. 7-9/2001.

[18] Debray, Regis (2002) Schimbarea ordinii globale (coordinator: Nathan Gardels), Antet.

PERSPECTIVES ON INTEROPERABILITY INTEGRATION WITHIN NATO DEFENSE PLANNING PROCESS

Florian CIOCAN

Field and Air Defense Training Center "Ioan Voda", Sibiu, Romania

Interoperability is not a new area of effort at NATO level. In fact, interoperability and more specifically standardization, has been a key element of the Alliance's approach to fielding forces for decades. But as the security and operational environment has been in a continuous change, the need to face the new threats and the current involvement in challenging operations in Afghanistan and elsewhere alongside with the necessity to interoperate at lower and lower levels of command with an increasing number of nations, including non-NATO ISAF partners, NGOs, and other organizations, have made the task even more challenging. In this respect Interoperability Integration within NATO Defense Planning Process will facilitate the timely identification, development and delivery of required forces and capabilities that are interoperable and adequately prepared, equipped, trained and supported to undertake the Alliance's full spectrum of missions.

Key words: *capability, defense planning process, interoperability*

> *"I see interoperability as taking first place: it is called a force multiplier. To me, interoperability means making our existing capabilities interoperable, as well as making sure the future ones will be. This pragmatism calls for closer coordination with nations, notably in developing and implementing capability improvements for forces preparing to deploy on operations."*
>
> General Stephane Abrial, Supreme Allied Commander Transformation

1. INTRODUCTION

NATO has been engaged in continuous and systematic transformation for many years to ensure that it has the policies, capabilities, and structures required in the changing international security environment to deal with current and future challenges, including of course the collective defense of its members. With Allied forces engaged in operations and missions across several continents, the Alliance needs to ensure that its armed forces remain modern, deployable, sustainable and thus interoperable [1].

In the old Cold War days, NATO was planning to defend against a Soviet attack by using what was called

a *"layered cake"* approach, namely National Corps after national Corps standing shoulder to shoulder, from the Baltic Sea to the Alps. Only at the boundary between those Corps, or in the case of reserve forces who might be called upon to reinforce the line, or break through to attack the enemy in the flanks, was interoperability much of an issue. But today, with the new NATO missions and engagement in operational theatres there has been a shift from a single nation fighting on its own to coalitions where multinational units, down to the level of platoons, are working together.

This reality has made achieving greater interoperability not just a *"nice to have"* but rather an essential element of NATO's operations which is also recognized as one of, if not the most important force multiplier.

In the meantime, it is important to stress what is the impact of the lack of interoperability. First, it can endanger operational mission success. Second, it can have a major negative impact on resources and on logistical footprint, as it makes it difficult, or even impossible, to share spare-parts, ammunition, fuel, and therefore affects the efficiency of the force, in general. But in certain areas non-interoperability can have a dramatic impact, like blue-on-blue fire or unnecessary loss of lives. That proves that enhancing interoperability improves the effectiveness of NATO operations and saves lives and resources.

As a result, of the need to improve interoperability within the Alliance, a NATO Interoperability Initiative was initiated with the main purpose to integrate interoperability in the new NATO Defense and Operations Planning Processes.

The new NATO Defense Planning Process will facilitate the timely identification, development and delivery of required forces and capabilities that are interoperable and adequately prepared, equipped, trained and supported to undertake the Alliance's full spectrum of missions. The Alliance will have to maintain existing and, in some cases, develop new capabilities, and adapt its structures to address the emerging security challenges and the changing character of war.

2. NATO INTEROPERABILITY INITIATIVE

2.1. ACTION PLAN FOR ENHANCING INTEROPERABILITY (APEI)

At the April 2008 Bucharest Summit, the heads of state and government directed the North Atlantic Council to review and recommend ways of improving the state of interoperability within the Alliance. In the first stage of this effort, formally known as the Action Plan for Enhancing Interoperability (APEI), key NATO defense planning committees and the NATO military authorities (NMAs) completed a questionnaire on the current and projected state of interoperability within their areas of responsibility.

Nations were invited to provide input as well.

The results of Phase I reported in spring 2009 were not surprising. Widespread shortfalls in interoperability exist across many capability areas within nations, between national forces, and among national and NATO forces and their systems and equipment. The most critical shortfall identified by the NMAs was the inability to communicate at all levels of command, caused by a combination of human factors, such as lack of language skills, and the lack of interoperable equipment. The NMAs also identified shortfalls in equipment, logistics, education, training, and doctrine.

Respondents from NATO and its allies agreed that the mechanisms for achieving interoperability are poorly understood and that one of the causes of insufficient interoperability was the nations' failure to implement agreed-on NATO standardization agreements (STANAGs). At the same time, the Phase I report concluded that the need for real and effective interoperability among nations is increasing as NATO operations become more expeditionary, ad hoc, and dynamic and as nations and NATO migrate to a network enabled operational environment. Though its initial conclusions echoed prior to interoperability assessments, the APEI is the first to involve all key stakeholders and NATO processes. Moreover, it has a mandate to provide regular progress reports to the defense ministers of NATO nations.

Phase II of the APEI, which began early in 2009, was aimed at identifying solutions and developing implementation plans. As part of this task, the NMAs and lead committees are reviewing and prioritizing NATO interoperability shortfalls, with a focus on short-term solutions. At the same time, the Phase I report noted that interoperability is inherently a long-term challenge that must be addressed as part of a new or adapted NATO defense planning process, not as a standalone process. A critical element of such a long-term approach is the identification of interoperability requirements and the validation of interoperability solutions. Tellingly, the Phase I report also highlighted the long-term need to facilitate national implementation of NATO STANAGs and Allied publications.

Additional Phase II work also included tasks related to the development of a long-term plan to resolve remaining interoperability shortfalls and the revision of the NATO policy for interoperability.

The APEI is bringing badly needed high-level attention and an operational perspective to the management of NATO interoperability, and it has the potential to formalize and nest interoperability planning within NATO's core defense planning processes. The on-going and prospective efforts to prioritize interoperability shortfalls and identify long-term interoperability requirements are crucial to the ultimate success of the APEI, and these need strong political and

technical support from each single member nation.

In order to implement APEI several tasks were established by the Secretary General for relevant NATO Committees, bodies and NMAs, as follows:

- To revise the NATO Interoperability Policy, including the definition of interoperability and to develop and coordinate the reviewing process;
- To ensure that long term interoperability will be addressed through its full integration into the NDPP and not as a separate standalone process, and that interoperability requirements are made an integral part of the NATO Capability Target within NDPP;
- To develop a plan for continuous review of the implementation status of STANAGs.

2.2. NATO INTEROPERABILITY POLICY REVIEW PROCESS

As a first step, the reviewed NATO Interoperability Policy superseding the earlier Policy on Interoperability CM(2005)0016 introduced the following elements: a changed definition for interoperability which was more general and more practical and viewed the concept as an integral part of the NATO defense and operations planning processes, and not a separate process, as well as the principles of interoperability [2].

Approved in December 2009, the Policy was complemented by a Strategy for Enhancing Interoperability that provides the necessary guidance for the implementation of the policy, covers the interim period until the NDPP is fully implemented and defines objectives, methods, tools, coordination and responsibilities. These documents have set the scene for the follow-on work, explaining the why, what, who, when and how of the Alliance's efforts to develop the underpinning elements of interoperability.

A key aspect of the new policy is the new definition of NATO interoperability: *"Interoperability is the ability to act together, coherently, effectively and efficiently to achieve Allied tactical, operational and strategic objective"* [3].

The new policy identifies several important principles: holistic approach to the achievement of interoperability, completeness and level of detail, consistency and coherence, timeliness, level of ambition, continuity of effort and commitment and application.

Also the policy stated that achieving meaningful interoperability supposes coordinated and sustained effort in the following areas: definition of interoperability requirements, identification of interoperability solutions, implementation of all parties agreed solutions and the test and validation of fielded solutions. All of these areas will be covered in detail within the fourth chapter of this paper, **"Interoperability Integration within NATO Defense Planning Process".**

Standardization will continue to be a key element in achieving interoperability. Hence, Nations and NATO bodies will continue to develop, approve, and collectively implement Allied standards. Other additional methods that could concurrently be applied include:

- Assuring close linkage between operational certification of forces prior to deployment and interoperability tests;
- Making better use of NATO common funds, multinational and civil-military approaches and encouraging nations to commit time and resources to improve interoperability, in addition to implementing agreed standards;
- Strengthening national commitment to information sharing, particularly in the deployed operations environment, to include, through the lessons learned process and NATO's relationship with industry, the definition and fielding of interoperability solutions.

As such, the lead committees and NMAs play an essential role by continuously and permanently addressing interoperability within their respective planning domains.

The various tools available for achieving interoperability should be selected in accordance with the specific dimension addressed (as identified in NATO Interoperability Policy, *i.e.* the technical, procedural, and human dimensions, including information as a cross-cutting element) and used either individually or in combinations as follows: standardization, training, exercises, education and evaluation, lessons learned, cooperative programs (*i.e.* multi-national, NATO common funded), and technical and other kind of demonstrations, trials, tests.

3. OVERVIEW OF THE NATO DEFENSE PLANNING PROCESS

3.1. EVOLUTION OF DEFENSE PLANNING WITHIN NATO

In essence, defense planning existed during the Cold War but *"operational planning"*, in the sense currently used, did not. This was because it was the task of force (and nuclear) planning to identify all the forces required to implement the collective defense war plans and members were expected to assign and employ the requested forces virtually without any questions asked. These war plans were, actually, the only *"operational plans"* of the era.

When, after the Cold War, the Alliance started to get involved in non-Article 5 operations, the situation had to change. Since these missions are, by agreement, case-by-case and the provision of national forces is discretionary, the automaticity of availability associated with force planning during the Cold War period was lost. This led to the requirement for *"force generation conferences"* to solicit the necessary forces and *"operational planning"* to develop the plans.

Existing processes were adjusted so that "defense planning" disciplines no longer focused exclusively

on meeting collective defense requirements and the needs of static warfare. Forces, assets, capabilities and facilities had to be capable of facing threats posed by failed states, ethnic rivalry, the proliferation of weapons of mass destruction and terrorism. In fact, acknowledging the ever-changing situation and recognizing the benefits of harmonization and coordination, the existing procedures were reviewed on a regular basis and adjusted as appropriate.

In practical terms, there was no standard defense planning process or defense planning cycle per se. Each of the seven principal disciplines was managed by a different NATO body and applied special procedures. They also contributed differently to the overall aim of providing the Alliance with the forces and capabilities to undertake the full range of its missions.

With the differences between the various components of the defense planning process and interrelated disciplines, the need for harmonization and coordination is essential.

While force planning had provided, to a certain extent, a basis for this harmonization and coordination, at the Istanbul Summit NATO leaders concluded that more was required. They directed the Council in Permanent Session to produce comprehensive political guidance in support of the Strategic Concept for all Alliance capabilities issues, planning disciplines and intelligence, responsive to the Alliance's requirements. They also directed that the interfaces between the respective Alliance planning disciplines, including operational planning, should be further analyzed.

With the adoption of a new Strategic Concept in November 2010 at the Lisbon Summit, Alliance leaders committed *"to ensure that NATO has the full range of capabilities necessary to deter and defend against any threat to the safety and security of NATO member states' populations"*[4].

Furthermore, the Alliance's 2010 Strategic Concept sets out NATO's strategic priorities and defines the organization's vision of Euro-Atlantic security for the next decade. It provides an analysis of the strategic environment and a framework for all Alliance capability development planning disciplines and intelligence, identifying the kinds of operations the Alliance must be able to perform and setting the context within which capability development takes place.

Defense planning, on the other hand, takes a more systematic approach and has a medium and longer-term perspective, including requirements identification, capabilities development and delivery, military and civilian structures adjustment personnel issues, equipment procurement and the development of new technologies.

A package of capabilities representing the Alliance's most pressing capability needs was endorsed at the Lisbon Summit. The

package goes hand in hand with and underpins the new Strategic Concept. It was developed to help the Alliance meet the demands of on-going operations, face emerging challenges and acquire key enabling capabilities. The package is based largely on existing plans and programs, as well as on a realistic projection of resources. It therefore provides a renewed focus and mandate to ensure that in the competition for resources the most urgent capabilities are delivered.

3.2. IMPLEMENTATION OF THE NEW NATO DEFENSE PLANNING PROCESS

In April 2009, NATO leaders endorsed the Outline Model of the new NATO Defense Planning Process. The latter aims to improve the harmonization of the planning domains, including their related committee structure and staffs, and encourage member countries to harmonize and integrate their national defense planning activities so as to complement NATO efforts. In his introductory remarks to defense ministers in June 2009, Jaap de Hoop Scheffer, NATO Secretary General at the time, underlined:

"If successfully implemented, the NDPP will mark the most profound change to defense planning in decades and has a very high potential to deliver tangible practical results". [4]

In the meantime, defense ministers endorsed the Implementation and Transition Plan of the NDPP. The NDPP introduces the concept of a more coherent and comprehensive defense planning process. It applies a specific approach and mechanism through which NATO is bringing its civilian and military side closer together engaging them in a common, functionally integrated approach to the issue of defense planning.

This has two major implications. Firstly, work will have to be done in a functionally integrated manner while at the same time ensuring that products are fully coordinated, coherent, persuasive, clear, and result-oriented and delivered on a timely basis. This has required a cultural shift in the way in which the HQs and staffs conduct business, particularly between the civilian and military experts and the various staffs supporting the committees responsible for the planning domains. Consequently, the demand for communication, consultation, coordination and for finding feasible and realistic solutions which are supported by all stakeholders is increasing.

Secondly, Allies themselves, in the delegations at NATO HQ and in capitals, have to exploit the full potential of the NDPP and coordinate and consolidate expert community views prior to presenting them in the various NATO fora. In this respect, it is crucial that individual members speak with one voice in the various NATO committees.

Therefore, the NDPP provides a framework within which national and

Alliance processes can be harmonized to meet Alliance objectives. It establishes in detail how to meet the mandates of the political guidance and sets targets for nations and the Alliance collectively, thereby guiding national and collective capability development. Implemented in a four-year cycle, the NDPP seeks forces and capabilities that are deployable, sustainable and can contribute to the full range of Alliance missions, allocating the totality of the Alliance's requirements to nations on the principles of fair burden sharing and reasonable challenge. The forces provided by Allies have to be able to operate together in a multinational context, prepared, trained, equipped and supported to contribute to the full range of missions, including in distant and remote areas.

3.3. NATO DEFENSE PLANNING PROCESS FRAMEWORK

Defense planning in the Alliance is a crucial tool which enables member countries to benefit from the political, military and resource advantages of working together. Within the defense planning process, Allies contribute to enhancing security and stability, and share the burden of developing and delivering the necessary forces and capabilities needed to achieve the Organization's objectives. The defense planning process prevents the renationalization of defense policies, while at the same time recognizing national sovereignty [5].

The aim of NATO defense planning is to provide a framework within which national and Alliance defense planning activities can be harmonized to meet agreed targets in the most effective way. It aims to facilitate the timely identification, development and delivery of the necessary range of forces - forces that are interoperable and adequately prepared, equipped, trained and supported - as well as the associated military and non-military capabilities to undertake the Alliance's full spectrum of missions [6].

The NDPP consists of five steps: establish political guidance, determine requirements, Apportion requirements and set targets, facilitate implementation, and review results. Although the process is sequential and cyclical in nature (four year cycle with bi-annual elements), some elements occur at different frequencies and implementation is a continuous activity.

The first step (Establish Political Guidance) provides the overall aims and objectives to be met by the Alliance within the framework of Alliance defense planning. It clearly defines what the Alliance should be able to do in broad quantitative and qualitative capability terms as well as the associated priorities. Political guidance should reflect the political, military, economic, legal, civil and technological factors which could impact on the development of the required capabilities. It will, inter alia, aim at defining the number, scale and nature of the operations the Alliance should be able to conduct in the future (commonly referred to as NATO's Level of Ambition)

The next step (Determine Requirements) consists in a comprehensive and detailed analysis in order to identify the capabilities required to achieve its Level of Ambition (LoA) and to steer capability development efforts of Allies and within NATO.

Thereafter comes apportioning the requirements to nations and setting targets for them, on the basis of fair burden sharing and reasonable challenge. These targets can be met either individually or multinationally. In addition, some targets or appropriate elements thereof can be assigned for collective (*i.e.* NATO common - funded) implementation.

The fourth step, Facilitate Implementation, as stated before, is a continuous activity. This step seeks to acquire the capabilities required by the Alliance by monitoring and encouraging national implementation, by facilitating and supporting multinational implementation and by executing collective implementation.

Finally, the fifth step, Review Results, seeks to examine the degree to which the aims and objectives set out in the NATO Political guidance and the associated targets have been met. It also seeks to assess the ability of NATO to meet its ambitions, and to offer feedback and direction for the defense planning process and its associated activities for the next cycle and/or any necessary mid-term and out-of-cycle actions.

The detailed model for the NATO Defense Planning Process is presented in **Diagram 1**.

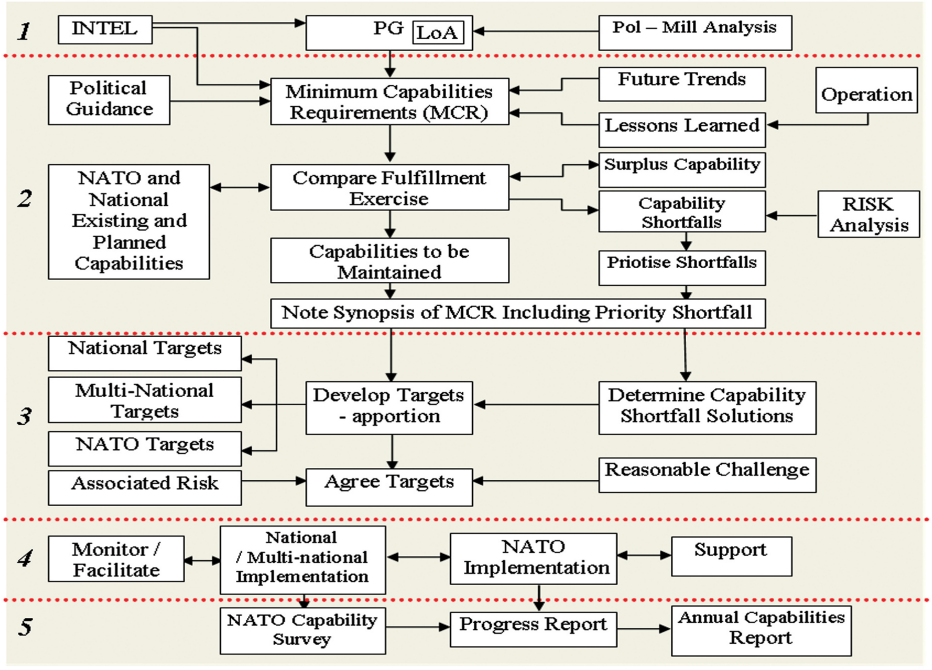

Diagram 1: The Outline Model For the NATO Defense Planning Process [7]

Furthermore the NDPP consist of several processes that allow the development and/or improvement, allocation and implementation of the capability.

The first one is Capability Requirement Review, formerly known as Defense Requirement Review, which is the analytical process and the associated support tool set used by the SCs that support all related planning domains to determine the Minimum Capability Requirement needed by the Alliance to meet its Level of Ambition and other agreed objectives set out in political guidance. Its construct has to logically and convincingly lead to the apportionment of identified requirements and their translation into capability targets which support nations in harmonizing their plans with NATO targets and priorities.

In order to be credible, reliable and transparent with respect to nations, the CRR adopt a capability-based approach by describing first the way NATO would conduct its operations in the future, and deriving from this description the functions that would have to be performed and the capabilities needed to support these functions.

The second one is Set Targets, formerly known as Force Planning. Initially the process includes the apportionment of the overall set of Minimum Capability Requirements to nations in the form of target packages for the delivery of required capabilities and mitigation of shortfalls while respecting the principles of fair burden sharing and reasonable challenge. It also includes the development of targets to be implemented by using common funding. This step in the process is a quadrennial effort, although the possibility for the introduction of out-of-cycle targets will be retained to remain responsive to the needs of the Alliance and individual Allies. Similarly, the option of a full revision or an update at the mid-term point will be retained to react to a change in the security environment or a change in political guidance.

Last but not least, the NATO Capability Review, or Defense Review, scrutinizes and assesses allies' defense and financial plans, as well as their collective efforts with a view to providing an overall assessment of the degree to which the combined forces and capabilities of the Alliance are able to meet the political guidance, including the NATO Level of Ambition. In addition, the NCR provides a key mechanism for generating feedback, any associated recommendations, and input to the next cycle.

4. INTEROPERABILITY INTEGRATION WITHIN NATO DEFENSE PLANNING PROCESS

As stated before, the Action Plan for Enhancing Interoperability Phase I report noted that interoperability is inherently a long term challenge that must be addressed as part of a new NATO defense planning process, not as a standalone process. In this respect, a critical element of such a long- term approach is the

identification of interoperability requirements and the validation of interoperability solutions.

Achieving interoperability is a shared responsibility of all stakeholders involved (including NATO staffs, lead committees for planning domains, NMAs, and in particular nations) and requires a constant and comprehensive coordination of all efforts between them.

In order to achieve meaningful interoperability, the following 4 areas listed in the NATO Interoperability Policy must be integrated into the NATO Defense Planning Process:

- Definition of interoperability requirements;
- Identification of interoperability solutions;
- Implementation of interoperability solutions;
- Test and validation of fielded solutions.

In the meantime, interoperability must be addressed systemically and continuously during the NDPP and may need to concentrate on certain areas in greater detail. The appropriate level of detail has to be defined by the relevant planning domain and the lead committee responsible.

To begin with, the Political Guidance that establishes in broad terms what the Alliance should be able to do, how much it should be able to do, as well as sets priorities, thereby guiding procurement and other key activities in the context of the NDPP is developed in the first step of NDPP. This Policy will provide the necessary information and guidance for the further development of the Guidance for Defense Planning (GDP). In its content GDP will include a specific chapter providing detailed guidance on the methodology, techniques and tools to be used in order to enable interoperability integration within NDPP.

Then, on NDPP step 2, during the Capability Requirement Review process, Strategic Commands will identify the requirements and associated shortfalls, with all planning domains joining in the analysis, in order to develop the single set of required Capabilities, the so called Minimum Capability Requirements (MCR) that will be made available to Nations. The complete set of capabilities needed by the Alliance to meet its Level of Ambition and other agreed objectives set out in political guidance will constitute the Minimum Capability Requirements, formerly referred to as Minimum Capability Requirements. They will also cover other areas such as Long Term Capability Requirements (LTCRs) and interoperability requirements. As such, during the Capability Requirement Review, together with the requirements derivation, the requirements for interoperability concerning in particular the ability to communicate operate and support will be defined / determined by the appropriate authorities / NMAs, and lead committees within their respective planning domains.

After that, on NDPS step 3, during the Set Targets process, interoperability solutions – expressed in standardization requirements,

lessons learned, training and education, procurement, etc. – will be developed based on the interoperability requirements defined before, and will be integrated into the targets.

These solutions will further support the next NDPP step in order to facilitate the implementation process. Nations and NATO bodies have responsibility for the implementation of agreed interoperability solutions. They also have the responsibility for certification and validation of the implemented solutions.

Standardization solutions for interoperability requirements will continue to be a key element in achieving and maintaining interoperability. These solutions, further developed into standardization requirements and documents, will continue with the development and implementation of concepts, doctrines, and procedures in order to achieve and maintain the required levels of compatibility, interchangeability or commonality in the operational, procedural, material, technical and administrative fields to support interoperability. The latter provides a main contribution to the combined operational effectiveness of the forces of the Alliance and supports the better use of economic resources. As such, Nations and NATO Bodies will continue to develop, approve, and collectively implement Allied Standards.

Finally, the plan for continuous review of the implementation status of STANAGs is the first step towards integration of interoperability, and of

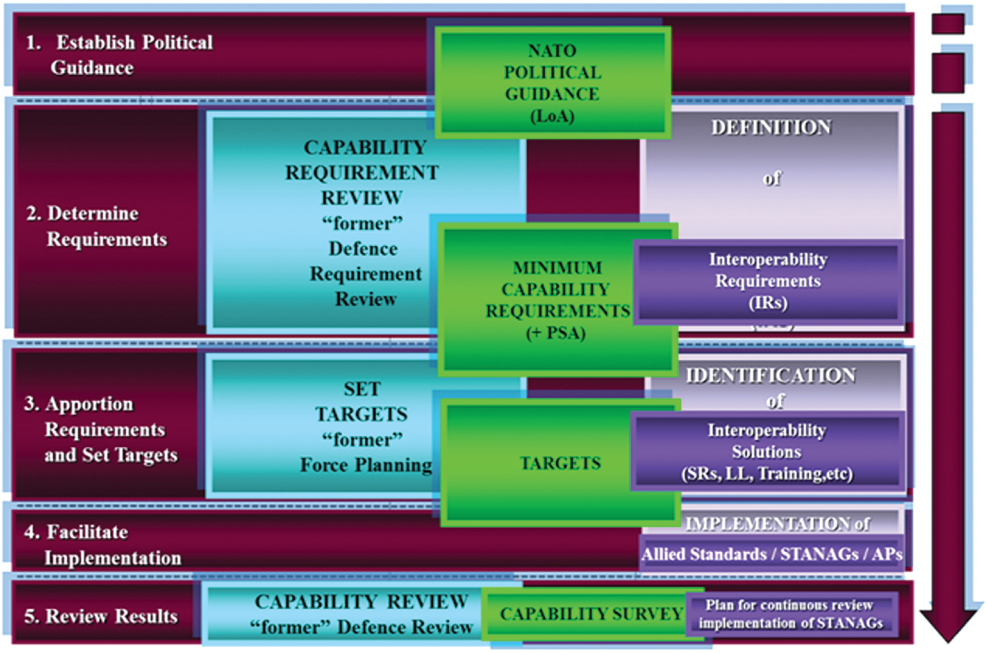

Diagram 2: Interoperability integration throughout the NATO Defense Planning Process

the related elements of standardization, in NATO Defense Planning Process.

As part of the NATO Capability Review process, the Capability Survey has a special chapter addressing interoperability, including the review of the continuous implementation status of Allied Standards/STANAGs. The Nations' responses provide useful information regarding the progresses made in the process of standards implementation and include proposals to improve the process of production, maintenance and management of NATO standardization documents.

The integration of interoperability throughout NATO Defence Planning Processes is illustrated in **Diagram 2**.

To sum-up, achieving interoperability is a continuous and coordinated effort at Alliance's level to enhance the effectiveness and efficiency of joint and multinational capabilities - designed, developed, implemented and improved within the NATO Defense Planning Process framework - required to support the full range of Alliance missions. Moreover, it is a shared responsibility of all stakeholders involved (including NATO staffs, lead committees for planning domains, NMAs, and in particular Nations) and requires a constant and comprehensive coordination of all efforts between them.

5. CONCLUSIONS

NATO is transforming itself to adapt to the challenges of the new and emerging security environment. The achievement of Alliance's objectives, in particular in operations, largely depends on the smooth and close cooperation between national, multinational and NATO assets.

NATO forces must have the capacity to defend Alliance territory, undertake demanding missions at strategic distance, contribute to a more secure international environment, and respond to unpredictable contingencies when and where that is required. Thus, there is a permanent need to transform NATO forces from the powerful but static posture of the Cold War into a posture that is more flexible, mobile, and versatile. With resources stretched thin in almost every NATO capital city, the Alliance must also make a firm commitment to smarter spending through a variety of efficiency and reform measures.

But to properly use existing and futures capabilities to confront these and many other challenges, a major issue that NATO and the NATO nations are working to contend with is interoperability.

Interoperability is not a new area of effort at NATO. In fact, interoperability has been a key element of the Alliance's approach to fielding forces for decades. But as the security and operational environment is continuously changing, the need to face the new threats and the current involvement in challenging operations, with the need to interoperate at lower and lower levels of command with an increasing number of nations, including non-NATO partners, NGOs, and other organizations, have made the task even more challenging.

An important element of the NATO continuous transformation process is interoperability. The latter

is recognized as a force multiplier and a key factor in increasing the military effectiveness of Allied forces and as an integral part of the NATO Defense Planning Process As such, it will support the identification, development and implementation of appropriate further capabilities and improve the existing ones. Thus, NATO will be enabled to adapt and respond to the new challenging security environment. Even if the framework and responsibility of integration are presented in the reviewed NATO Interoperability Policy and Strategy, methodology and details on how to fulfill this challenging task are still under the concept and development phases.

In this respect, this paper provided a perspective on how the process of interoperability integration within NDPP should take place, based on the key documents already approved, as well as on the assumptions and on the on-going developments and activities.

ENDNOTES

[1] http://www.nato.int/cps/en/SID-34742C8F-15AB D2DD/natolive/topics_49137.htm.

[2] Interoperability Documents for Inter-Committees Coordination, C-M(2009)0145, page 1 http://www.tradoc.mil.al/Standartizimi/Downloads/C-M(2009)0145.

[3] Idem.

[4] Active Engagement, Modern Defence - Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation, pag.15, para. 19.

[5] The NATO Defence Planning Process: http://www.nato.int/ops/en/natolive/topics_49202/htm.

[6] Idem.

[7] Bi-SC Priority Shortfall Areas, NATO, May 2009, Annex B.

REFERENCES

[1] Active Engagement, Modern Defense - Strategic Concept for the Defense and Security of the Members of the North Atlantic Treaty Organization, Public Diplomacy Division, NATO, 2010, Brussels, Belgium: www.nato.int-www.nato.int/ebookshop.

[2] Bi-SC Priority Shortfall Areas, NATO, May 2009: www.nfgm.gov.hu/data/cms2019245/12_BiSCPSADECLASUS_Final.pdf.

[3] Holger Pfeiffer - Defense and Force Planning in Historical Perspective: NATO as a case study, Baltic Security & Defense Review, Volume 10, 2008: ebookbrowse.com/5-holger-pfeiffer-defence-and-force-planning-in-historical-perspective-nato-as-a-case-study-pdf-d28466265.

[4] Improving NATO's Capability: http://www.nato.int/cps/en/SID-4742C8F-15ABD2DD/natolive/topics_49137.htm.

[5] Interoperability Documents for Inter-Committees Coordination, C-M(2009)0145 http://www.tradoc.mil.al/Standartizimi/Downloads/CM(2009)0145%20%20(NATO%20POLICY%20FOR%20INTEROPERABILITY%20AND%20STRATEGY).pdf.

[6] NATO Glossary of Standardization Terms and Definitions - AAP - 42: http://www.nato.int/docu/stanag/aap042/2007-aap42.pdf)

[7] NATO Handbook, Public Diplomacy Division, NATO, 2006, Brussels, Belgium: www.nato.int-www.nato.int/ebookshop)

[8] Outline Model for a NATO Defense Planning Process, PO(2009)0042

[9] The NATO Defense Planning Process: http://www.nato.int/ops/en/natolive/topics_49202/htm)

STRATEGIC AIRLIFT CAPABILITY: FROM THEORY TO PRACTICE

Cezar VASILESCU

Senior lecturer, PhD eng., Regional Department of Defense Resources Management Studies, Brasov, Romania

Strategic airlift remains a critical supporting capability that should be achieved, maintained and improved. This capability ensures the ability to deploy and sustain military forces across possible distant battlefields. The paper analyses the growing strategic airlift capabilities gap between operational needs and current realities, and underlines the need for an enhanced strategic airlift capability to meet current and future NATO alliance needs. By analyzing requirements against the existing/potential solutions, this paper further ponders over options like the organic national capability, partnerships such as the Strategic Airlift Consortium (SAC) or leasing aircraft through a venture such as the Strategic Airlift Interim Solution (SALIS). The paper also evaluates the feasibility of applying these solutions to European Union airlift needs.

Key words: *Strategic Airlift Consortium (SAC), Strategic Airlift Interim Solution (SALIS), strategic airlift capability, NATO Critical Capabilities Package.*

"Systematic use of pooled and shared assets would reduce duplications, overheads and, in the medium-term, increase capabilities".

1. INTRODUCTION

The global security interests suggest that the principal tasks for the armed forces over the next 25 years will remain much as they have been, but potentially with intensified demands. War related or peace keeping missions will be the starting point for choosing the national or multinational military capabilities. Those capabilities required for a large range of possible operations in different regions will allow nations to make a credible contribution to regional stability.

Over the time, national armed forces need to remain interoperable with main partners and allies. It will also need to be deployable, sufficiently self-reliant, versatile, and adaptable. Their international interests require that nations must retain the ability to contribute with combat capabilities when required. The general result

should be a projected force structure that retains and enhances its current mix of capabilities, enabling it to operate in places similar or different to where it is today.

In this respect, strategic airlift remains a critical supporting capability that should be achieved, maintained and improved. This capability ensures the ability to deploy and sustain military forces across possible distant battlefields.

The combat effectiveness, protection, sustainability, and mobility of military forces are highly important objectives, and that's why the enabling capabilities of long-range air transport are so critical.

Generally speaking, the term capability is used to describe the personnel, equipment, platforms and/or other material that affect the capacity to undertake military operations. More specifically, capability is:

"The power to achieve a desired operational effect in a nominated environment, within a specified time, and to sustain that effect for a designated period. Capability is generated by some fundamental inputs such as organization, personnel, collective training, major systems, supplies, facilities, support, command and management". [1]

Airlift capability represents *"the total capacity expressed in terms of number of passengers and/or weight/ cubic displacement of cargo that can be carried at any one time to a given destination by available airlift"* [2]. It consists of two distinct types, strategic and tactical airlifting. Typically, strategic airlifting involves moving materiel, weapons and personnel over long distances (across or off the continent or theater), whereas a tactical airlift focuses on deploying resources and material into a specific location with high precision.

Military strategic transport aircraft are distinguished by their load capacity (cargo and passengers) that they are able to carry and by the distance (range) they can cover. Strategic airlifters are generally larger and can fly longer distances than tactical ones.

Aircraft which perform this role are considered strategic airlifters, such as Lockheed C-141 Starlifter, Lockheed C-5 Galaxy, Boeing C-17 Globemaster III, Ilyushin Il-76 Candid or Antonov An-124 Ruslan, in contrast with tactical airlifters, such as the C-130 Hercules, Lockheed Martin C-27 Spartan and Transall C-160, which can normally only move supplies within a given theater of operations.

Table 1 presents a comparison of strategic airlifters based on capacity and range, flown at full load and without air-to-air refueling (where is the case) [3].

In the context that we are talking about, the desired strategic aircraft should be based on aircraft that have the capacity not only to fly long distances, but also to carry oversized and overweight equipment.

Table 1. A comparison of strategic airlifters based on capacity and range.

Type	Aircraft	Capacity [tones]	Range [km]
Medium size	C-160 Transall	16	1,800
	C-130 Hercules	17	3,200-5,000
Outsize medium	A 400M	35	3,700
	AN-70	47	1,350
	Ilyushin IL-76	47	3,000
	C-17 Globemaster	80	5,000
Outsize upper	C-5 Galaxy	120	5,200
	AN-124	135	5,000

2. ACHIEVING STRATEGIC AIRLIFT CAPABILITY

Achieving strategic airlift capability is a question of funding, military strategy and economic efficiency analysis. United States has currently the greatest strategic airlift capacity in the world, while many countries' armed forces possess little or none.

NATO and EU can rely on three primary options, either individually or in combination, to increase airlift capacity:

1. increased organic national capability,
2. leasing aircraft through a venture such as the Strategic Airlift Interim Solution (SALIS) or,
3. purchasing aircraft under a partnership such as the Strategic Airlift Consortium (SAC).

Hereinafter, we will analyze each of the three options. The Movement and Transportation Principles section of the "NATO principles and policies for movement and transportation" document states "nations are responsible for obtaining transportation resources to deploy, sustain and redeploy their forces" [4].

The United States currently operates 52 C-5B/C/A model aircraft, five C-5M Super Galaxy [5] and 211 C-17 Globemaster III aircraft [6]. Great Britain now owns five C-17 aircraft and Canada recently took delivery of their fourth C-17.

In addition to the recent British and Canadian C-17 procurements, the European consortium Airbus produced the first prototype A400M aircraft in June 2008. Airbus plans to build and deliver (until 2020) 180 A400M aircraft for eight NATO members: Germany (60), France (50), Belgium (7), UK (25), Spain (27), Luxembourg (1), and Turkey (10).

Canadian Forces (CF) also requires strategic airlift support and air mobility to ensure the effectiveness and rapid deployability of forces independently or jointly in Coalition, United Nations or NATO operations. The Strategic Airlift Capability Project observed that Canada's increasing requirements were served by a mixture of military and commercial aircraft [7].

The CF military airlift capability was provided by 32 CF CC-130 Hercules, five CC-150 Polaris aircraft and commercial contracted airlift. But CC-130 Hercules (acquired in 1964-1968 timeframe) can provide only limited strategic airlift capability and capacity. The limitations relate to the long distances involved in strategic airlift, cargo volume constraints and slower flying speeds. Moreover, the

retirement in 2010 of up to fourteen older Hercules aircraft reduced the level of service to unacceptable levels.

The Strategic Airlift Capability Project noted that these assets will not been able to satisfy CF airlift requirements and are not expected to meet the required strategic airlift needs in the future. A strategic airlift capability (called Strategic Air Transport - SAT Weapon System) should be procured as part of an integrated and unified approach to airlift to permit the CF to be a more effective, relevant and responsive force, interoperable with CF allies, particularly NATO and the US Air Force (USAF).

New Zealand chooses the approach of having a small (but adequate) airlift capability [8], based on a fleet of the two B757 and an ongoing upgrade program for the existing five C-130H Hercules aircraft. The initiative is considered vital to maintain NZ independent airlift capability, and will be augmented on medium term (2020) with a replacement aircraft program. The decision on the appropriate replacement will be based on a study that will be finished before the next Defense Review (around 2015).

Alternatively, groups of nations (such as NATO members) choose to pool their strategic airlift resources rather than individually duplicating the substantial investment required to purchase and maintain such costly and, in many cases, seldom-used assets.

The November 2006 Riga summit noted that NATO is involved in six missions and operations on three continents, but some analysts termed strategic airlift as *"potentially the alliance's Achilles heel of capabilities"*.

There are several ongoing initiatives in NATO and EU to overcome deficiencies concerning strategic airlift capabilities. NATO Response Force needs this capability for expeditionary operations like the ongoing operations in Afghanistan, assistance in case of tsunami or earthquake occurrence or in Africa for UN humanitarian relief support operations.

In 2007, within the framework of the Strategic Airlift Capability (SAC) program, ten NATO member states (Bulgaria, Estonia, Hungary, Lithuania, Netherlands, Norway, Poland, Romania, Slovenia and United States) plus two partner countries (Sweden and Finland) decided to acquire, manage, support and operate three Boeing C-17 Globemaster III strategic transport aircraft [9]. The airplanes are available to participant nations for a number of pre-agreed flying hours and the permanent base is located in Papa Air Base in Hungary.

There are several issues to be overcome, such as:

- crews and support personnel need to be trained for mission profiles and standards agreed by all participating countries;
- the aircraft missions schedule should meet national requirements, but must also be accommodated to NATO, UN or EU missions;

In order to achieve the prompt fulfillment of the member countries' missions, SAC does not require the unanimous agreement of its partners for operations. Therefore, each nation "owns" a share of the SAC aircraft's flight hours that can be used for missions of interest to that particular nation. In contrast with this arrangement, the personnel contributed by each nation are assigned to various missions, not only those requested by their nation.

Currently, the aircraft is operated by aircrews from all participating nations under the command of a multinational military structure (Heavy Airlift Wing - HAW).

In May 2010 was declared Initial Operational Capability (IOC) of the HAW. Full Operational Capability (FOC) of the HAW is anticipated for late 2011 or beginning 2012. It will be declared when HAW will be able to conduct the whole range of missions assigned to it, having available the entire fleet of three C-17s.

A second initiative is the Strategic Airlift Interim Solution (SALIS), under which a multinational airlift consortium of 16 NATO countries (Belgium, Canada, Czech Republic, Denmark, France, Germany, Greece, Hungary, Luxembourg, Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, United Kingdom) plus two partner nations (Finland and Sweden) contracted six Antonov An-124-100 transport aircraft from a civilian company [10]. The airplanes are provided for the transportation of unusually large cargo as follows: two aircraft on full-time charter, two more on six days' notice and another two on nine days' notice.

The countries committed themselves to use the aircraft for a minimum of 2000 flying hours per year. The initial contract was signed on 2006 with Ruslan SALIS GmbH, a subsidiary of the Russian company Volga Dnepr, based in Leipzig and it expires on 31 December 2012.

The difference between SAC Program and SALIS is that in the first the countries that joined it have purchased the aircraft together, while in SALIS they just contract flight hours in a charter-like way. Based on their initial contribution to the program the SAC participants are entitled to a corresponding percentage of the available flight hours.

These two complementary initiatives are very important because:

- it gave the Alliance the capability to reach out globally and transport troops, equipment and supplies across the world;
- strategic airlift capabilities are vital to ensure that NATO countries are able to deploy their forces and equipment rapidly to wherever they are needed;
- by pooling resources, NATO countries made significant financial savings, and have the potential of collectively acquiring assets that otherwise would be prohibitively expensive to purchase as individual countries.

At the Lisbon 2010 Summit, NATO presented its new Strategic Concept that defines the Alliance's strategic

priorities for the next decade. As part of the strategic concept, a new "Critical Capabilities Package" was endorsed representing the Alliance's most pressing capability needs.

While the package was based mostly on existing plans and programs it assures that the most urgent capabilities are provided, helping the Alliance to face the demands of ongoing operations, emerging challenges and acquire key enabling capabilities. Once again, improving air- and sea-lift capabilities was mentioned on the list of Lisbon's Prioritized Capabilities Package [11].

An important aspect in relation with strategic airlift capability is the coordination issues among the "players". At present, both NATO's Strategic Airlift Coordination Centre and the EU's European Airlift Centre are co-located in Eindhoven [12].

In 2005, when the African Union asked both the EU and NATO to give logistical support to their peacekeeping mission in Darfur, both organizations decided to use separate airlift commands in Europe.

One step ahead on coordinating strategic airlift fleet was during EUROFOR operation in support of UN mission in place (MONUC) in its stabilizing role during the election process in Congo (2006). The airlift operation between Europe, Gabon and Kinshasa relied on SALIS (Strategic Airlift Interim Solution) system. Even it was an EU mission flights between Europe and Africa were coordinated by the Strategic Airlift Coordination Centre in Eindhoven, Netherlands, in liaison with the operational HQ.

3. CONCLUSIONS

The Strategic Airlift Interim Solution is very much an interim solution - the Antonovs have been leased to meet shortfalls in European strategic airlift capabilities, until deliveries of Airbus A400M aircraft begin, likely in 2010 [13].

The A400M is a collaborative effort involving governments and industry of eight Europeans countries and it is designed to satisfy the European requirement for rapid, reliable air mobility for force deployment and humanitarian missions, in peace, crisis and war situations. Even if the A400M is smaller than a C-17, it can transport two-thirds the volume and half of the payload at less than half of its price and at a third of its life-cycle costs [14].

Four European nations (Germany, France, Great Britain and Spain) plan to purchase 90% of the original A400M production. While this enhances a European capability, the numerous other European nations without A400M purchases will remain as dependent on their European neighbors as the alliance currently is on the United States.

The European Defense Agency is currently exploring with EU countries the possibilities of pooling acquisitions of additional aircraft, partnering in contracting transport services, and pooling maintenance and training in case of additional A400M procurement.

Relying on current US, British and Canadian capability does not solve the problems regarding developing European capability identified in the Prague Capabilities Commitment.

EU countries have to rethink their strategic military airlift approaches. Given that there is a lot of uncertainty over the factors that influence lift requirements probably nobody can give a definite answer on how much and what kind of airlift will be enough to cover the overgrowing nations' needs. Ultimately, decision makers must balance the costs involved in strategic transport investment against the capabilities that these assets will provide.

In operations where EU members participate alongside the US, to compensate the European deficiency in terms of airlift, the use of US aircraft is by no means guaranteed since these assets are barely sufficient for US own needs or they may need to use them elsewhere.

The reasonable question is if the handful of C-17s and leased Antonovs will provide enough strategic airlift capability for the EU's near-future operational requirements. The answer depends on what those requirements will be. The alternatives are either EU nations are not planning to extend their global military reach as much as first thought, or a more long-term strategic airlift capability will be required.

In 2010, the second Headline Goal for the establishment of rapid-reaction battle groups of combined European Union (EU) force expired. If in the future such force will prove itself useful and possible to be achieved, to ensure the effectiveness of these formations EU countries have to rethink their strategic military airlift approaches.

The original idea stated that each EU battle group, made up of around 1,500 combat troops plus support and combat support units, must be capable of operating 80 missions by C-130-sized transports. Each group should be sustainable from 30 days, extendible up to three months. The aim is for the battle groups to begin operations 10 days after a European Council decision on action.

For many nations in Europe this is a tough challenge. There is a chronic lack of strategic airlift capability across the EU, especially among smaller states, a problem that has been recognized for some time but for which only temporary solutions have so far been found. The issue is being addressed through a combination of national procurements, leasing, such as the multinational Strategic Airlift Interim Solution (SALIS) agreement, or by accessing strategic military transporters being made available within the NATO strategic airlift capability program.

There are at least six policy options to solve the complicated airlift capability deficit: long-term

procurement (joint production, off-the-shelf purchasing or long term leasing), short-term leasing and chartering, government-contractor agreements to use commercial lift assets, public-private partnerships, pooling and role specialization.

Each of these options has advantages and disadvantages [15] summarized hereinafter.

1. Long term procurement

Pros
- Greatest level of assured access and timeliness / responsiveness

Cons
- High cost
- Reduced flexibility
- Maintenance and other logistic support requirements

1.1. Joint production

Pros
- Economies of scale
- Gains from specialization
- Increased affordability for individual nations

Cons
- Delays
- Coordination issues
- Commitment issues

1.2. Off-the-shelf purchasing

Pros
- Wider choice
- Less costly than production
- Speedy acquisition

Cons
- Specifications may not always fit requirements
- Does not support EU defense industrial base and preservation of EU technical and industrial capabilities

1.3. Long term leasing

Pros
- Simpler acquisition than owning
- Assured access
- Financial benefits: avoids large initial capital outlay
- Support structure may be less costly than owning

Cons
- High cost (overall more expensive than ownership)
- Potential leasing restrictions on operational use of assets

2. Short term leasing and chartering

Pros
- Simpler acquisition than owning
- Allows long term control and assured access to assets and availability
- financial benefits
- support structure savings

Cons
- Expensive option
- Problems with timely access to assets for the immediate deployment phase, but may be adequate for later phases
- limited asset availability depending on requirement
- restriction related to security
- potential high insurance cost for operations in hostile environment
- quality/suitability problems
-diminished political control

3. Government-contractor agreements to use commercial lift assets

Pros
- less expensive than owning or leasing assets
- assured access to airlift capability provided

Cons
- costly retainer contracts
- problems with timely availability
- reluctance of commercial operators to go into dangerous situations
- suitability problems
- need for governments to provide strong incentives to attract interest of commercial carriers

4. Public-private partnerships

Pros
- financing advantages
- advantage from transfer to risk to private sector

Cons
-need to government to provide incentives to the private sector

5. Pooling

Pros
- flexibility - modules can be assembled in many ways
- less costly than national/ multinational purchase or lease
- political feasibility due to limited EU role

Cons
- coordination, module assembly may be complex
- requirement for nations to act promptly to make committed assets available in a timely way
- sovereignty and concerns over control

6. Role specialization

Pros
- potentially greater focus and competence through specialization

Cons
- politically controversial; division of labour require large amount of trust, willingness to relinquish national sovereignty
- potential complexity of role integration

The changing world needs the capabilities provided by the NATO alliance and the European Union. To meet challenging global demands, both organizations, and their component nations, require force projection capabilities. Strategic airlift provides the capability to extend the NATO and EU reach into trouble spots with the flexible options of humanitarian assistance to conventional military operations. Maximizing strategic airlift capability ensures NATO and the EU can initiate and sustain operations throughout the globe within challenging fiscal realities [16].

Improving strategic airlift capabilities creates a more capable NATO alliance by providing a common asset for all nations to employ. Small and large nations benefit from reduced acquisition costs, life cycle costs, while receiving the benefits of a greater pool of aircraft to meet national and alliance needs. Finally, developing strategic airlift capability enhances overall NATO capability no matter the outcome of current debates over collective defense versus collective security.

REFERENCES

[1] *** Defence Capability Development Manual, Defence Publishing Service, Department of Defence, Canberra, 2006.

[2] *** Department of Defense Dictionary of Military and Associated Terms, amended through 15 May 2011.

[3] K. Vlachos-Dengler - Getting there: building strategic mobility into ESDP, The European Union Institute for Security Studies, November 2002, pp. 17, 36-37.

[4] *** Allied Joint Movement and Transportation Doctrine AJP-4.4(A), NATO Standardization Agency (NSA), December 2005.

[5]***http://www.lockheedmartin.com/news/press_releases/2011/110412ae_second-production-c5m-delivered.html.

[6] *** http://www.boeing.com/defense-space/military/c17/.

[7] *** Strategic Airlift Capability Project - Statement of Operational Requirement, Department of National Defence, Canada, June 2006.

[8] *** Defence White Paper, New Zealand Ministry of Defence, November 2010.

[9] *** Defence Capability Development Manual, Defence Publishing Service, Department of Defence, Canberra, 2006.

[10] *** Strategic Airlift Interim Solution (SALIS), http://www.nato.int/cps/en/natolive/topics_50106.htm?selectedLocale=en.

[11] *** Improving NATO's capabilities, http://www.nato.int/cps/en/natolive/topics_49137.htm?selectedLocale=en.

[12] G. Grevi et. al. - *European Security and Defense Policy: The first 10 years (1999-2009)*, The European Union Institute for Security Studies, October 2009.

[13] Butterworth-Hayes, P. EU confronts strategic airlift shortfalls, AIAA Aerospace America, March 2007.

[14] *** *Strategic Airlift Capability Project - Statement of Operational Requirement*, Department of National Defence, Canada, June 2006.

[15] *** http://www.boeing.com/defense-space/military/c17/.

[16] J. D. Hood - *NATO Strategic Airlift: Capability or Continued US Reliance?,* Maxwell Air Force Base, April 2009.

[17] Carl Ek, *NATO's Prague Capabilities Commitment CRS Report*, Foreign Affairs, Defense, and Trade Division, July 22, 2008.

COMMUNICATIONS AND INFORMATION SYSTEMS IN SUPPORT OF EUROPEAN UNION-LED CRISIS MANAGEMENT MISSIONS

Dănuț ȚIGĂNUȘ

"Carol I" National Defense University, Bucharest, Romania

This essay assesses the communications and information systems (CIS) in support of the civilian and military structures deployed in the European Union led crises management operations and missions. The article emphasizes the specific structure and function of CIS taking in consideration the particularities of EU led missions. The integration of the EU institutional networks and systems with the national systems provided by the EU member states is considered a key element. The analysis-part of this paper starts with the specific EU command and control system for crises management missions based on two autonomous solutions and one relying on NATO capabilities. Further, it continues with the challenges of the classified information exchange at the operational theatre level. The most important contribution of this article is based on the long term vision implementation measures for the CIS structure, roles, functions and services provided and the information management infrastructure. CIS deployment mechanisms are described with references to the practical situation of the CIS deployed in support of crises management operations and missions. Two important definitions are provided regarding the CIS for crisis management and their roles in the specific EU operational environment. The system view of the operational CIS is depicted and analysed also, with a focus on the integration aspects of the infrastructure as the information transport layer for the information exchange flow. The last part of the article focuses on the CIS functions for the deployed systems which are detailed alongside with the C2 and Information Exchange Requirements in the EU operational environment. The variety of the theoretical approaches to determine the CIS infrastructure for EU-led civilian and military missions triggers the conclusion that the planning and implementation process is extremely complex especially in the context of the new security environment and requires national participation and adaptation of the national and institutional development programs in the CIS field.

Key words: *Communications and Information Systems (CIS), EU Common Security and Defence Policy, Information Exchange Gateway, Operational Headquarters (OHQ), Force Headquarters (FHQ), crisis management, EU-led missions.*

Unlike traditional military operations conducted by NATO or national armed forces in coalition operations, the diversity of operational scenarios in which communications and information systems (CIS) can be used for crisis management missions led by the EU produces an

essential element of specificity in the planning, implementation and use of these systems.

On the other hand, the different nature of command and control system in the Common Security and Defence Policy (CSDP), based on the ad-hoc solution chosen by the political decision-factor for each operational scenario and depending on the availability of the Member States to accept one of the seven existing command and control possibilities for EU-led operations, entails the establishment of similar CIS specific solutions from case to case. Mention should be made that five of these possibilities are offered by the United Kingdom, France, Germany, Italy and Greece, as strategic operational command posts (Operational Headquarters - OHQ) provided by a framework member state. Another option is implemented through EU Cell at SHAPE based on a Berlin Plus operation and resorting to NATO command and control capabilities. The EU Operation Center in Brussels could be activated by EU External Action Service and this is the third C2 option for an EU-led Crisis Management Operation.

The planning process shall apply to support the military strategic, operational and tactical headquarters and the institutional administrative and management system, including information exchange between these commands.

The same happens with the CIS in support of the civilian missions, the difference consisting in that the strategic management is carried out by the Civilian Planning and Conduct Capability (CPCC) which, acting as an operational command for all civilian ongoing EU-led missions, has continuously available communications and information systems to achieve the internal information flow and the communications with the operational theatres. In this case, the major problems of planning, deployment and implementation of the related CIS are related to the strategic communications with the operational theatres and, in particular, to the creation of the infrastructure in theatre for specific support of these missions.

It is important to note that the CIS for crisis management operations have to support both the functional and operational requirements, and the technical requirements (i.e. systems availability, efficient use of the hardware and software, availability of information, information security and interoperability with other similar systems).

To understand the organizational and procedural planning framework for communications an information systems in support of EU-led Crisis Management Operations (CMOs) we must first define their concept, role, structure, functions performed, criteria of engagement into the mission and the responsibilities of the specialised personnel in the operational environment.

Thus, the communication and information system for crisis management under Common Security and Defence Policy is defined, from a conceptual perspective, as a set

of basic and functional distributed components, organically interacting under the action of the human factor. Its primary objective is to facilitate the monitoring, early warning, operational planning, command and control and decision making processes in order to identify the measures, methods and procedures designated to bring a crisis situation under the national or international forces control and to allow the conduct of coordinated actions using civilian and/ or military instruments to return the situation back to normality.

Regarding the role of CIS, the literature in the field covers the following aspects: the role of staff and personnel, the operating procedures, the information management mechanism and the physical infrastructure needed for the support of decision making together with the aspects of planning, preparation, execution and evaluation of operations (Burlacu: 2007).

The EU institutions are involved in the monitoring of the operational situation in the area affected by the crisis and are responsible for the planning, preparation, execution and evaluation of a mission for crisis management. The EU Member States will provide the Headquarters, forces and the military and/or civilian means for deployment and intervention in the field. These forces must be supported by the CIS to perform efficient information flow directed at all hierarchical levels, from the political-strategic level down to the tactical level in the operational theatre.

The EU specificity requires a comprehensive approach in providing the SCI for the exchange of information between civilian and military entities acting for crisis management, in order to coordinate their efforts and the efficient use of all instruments that EU decides to commit to specific management of a crisis.

This approach is different from what is the Civil-Military Cooperation (CIMIC) or the corresponding principle of cooperation between NATO military forces and other forces or NGOs acting together to achieve desired effects and the operational objectives in a broader theatre security framework.

Hence, the role of the CIS in support of the crisis management practiced by the EU is to ensure the timely and effective information exchange within the command and control, cooperation and monitoring given its capacity to support the conduct of military and/or civilian action in the mission, the extension of the communication and information system from the permanent locations to the deployed locations outside the EU territory, and to ensure the necessary redundancy in order to allow the channels and services manoeuvre.

Communications and information systems will be based on complex, coherent and integrated network architecture, from commercial sources, national military and/or belonging to the EU, supported by a robust and sufficient infrastructure

which is formed from a series of mixed terrestrial and satellite communications in order to provide broadband capabilities for collecting, processing and disseminating data and information.

Based on this architecture, we can determine the structure of communications and information system for UE-led CMOs. This includes:

a) CIS with fixed infrastructure, consisting of the federalisation of the following components: IOLAN (Intranet Office Local Area Network - unclassified), SOLAN (Secure Office Local Area Network - classified), EU OPS WAN (EU Operation Wide Area Network), ESDP-NET (European Security and Defence Policy Network - formal messaging system for EU security and defense issues), Cortesy (COREU Terminal Equipment-general messaging system between communications centres), INTEL LAN (Intelligence Local Area Network), Extranet R (classified messaging system between EU and Member States), EU-TEL-SEC (EU encrypted telephone system), the OHQ and FHQ LANs in the permanent location.

b) CIS for surveillance and early warning: GMES (Global Monitoring for Environment and Security), Galileo (Global Navigation Satellite System), MARSUR (Maritime Surveillance System).

c) Deployable CIS consisting of: Operational Headquarters (OHQ) LAN, Deployed Force headquarters - (F)HQ, Deployable Packages (DP), EU command and control system (EU CCIS) and the CIS elements of the deployable Battlegroups (BGs).

d) CIS of the Member States: national integrated systems in support of crisis management, belonging to Member States.

The structure of the communications and information system for crisis management operations is presented in **Figure 1**.

The CIS for EU-led CMOs will have a modular and scalable structure, being organised with permanent communications and information centres (PCIC), installed in Brussels and in the capitals of the Member States, operational communications and information centres (OCIC), fixed and deployed, transit or end-user set up in the operational headquarters (OHQ, FHQ, components or BGs forces) and communications lines (CL) achieved in various transport media information (optical fibre, copper circuits, radio, radio relay, satellite).

This architecture will support the operational command and control (C2) option established at political-strategic level, and will provide the information exchange gateways for interconnection of the classified networks and domains as well as the CIS spare part usually established at 10% of quantitative active network equipment and terminals.

Based on this vision all elements will be integrated on the communications infrastructure

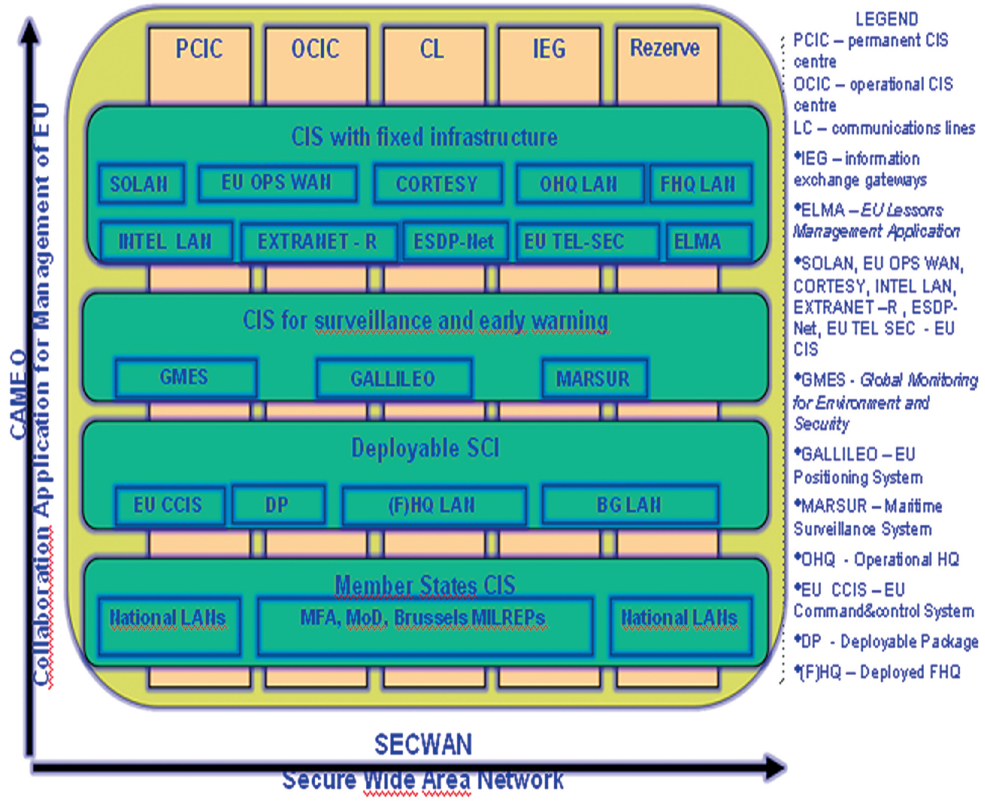

Fig. 1. *The structure of the CIS for EU-led Crisis Management Operations*

transport layer containing two classification domains, SECRET UE and RESTREINT UE. Both domains will be integrated on the EU SECWAN (EU Secure Wide Area Network) which is using CAMEO (Collaboration Application for Management of EU Operations) as a collaboration application for planning of EU-led operations.

From physical implementation perspective the CIS in support of CMOs are formed from three basis elements, as follows:

- Integrated network infrastructure for voice, date and VTC services. This infrastructure facilitates information flow and generates the optimal conditions for data exchange between various actors in the field;

- Hardware equipment as servers, terminal work stations and active network equipment needed for the system to maintain its operational status;

- Software elements: operating system, databases and applications, the logical storage and the client core and functional applications.

In terms of organizational structures, the implementation of efficient communications and information units, sub-units and formations should be based on scientific studies results (Timofte G, Tudose E., Vişan D: 2006, p. 70), as their set up will take into account the following elements:

- operational and technical conditions of employment of CIS in support of crisis management mission;
- experience and lessons identified from completed or ongoing operations in terms of CIS organizational structures;
- the number of users in the permanent and deployable command posts;
- the skills and knowledge of users and specialized technical assistance requirements during the CIS support;
- the number and the field deployable command posts;
- the time to install, make available and redeploy the CIS;
- the staff necessary to maintain viability, reliability and stability in the functioning of the CIS in terms of the engagement;
- the traffic volume estimated at maximum load times of the information flow;
- the need for interconnection with other communications and information systems, governmental structures or security units acting simultaneously in the operational theatre.

It is considered that for the installation, operation, removal and redeploy of the CIS in support of crisis management missions conducted by a brigade, there is a need to engage a CIS structure equivalent to a company, and for a battalion level there is a need for a platoon CIS level.

CIS will have modular structures and composition and will be organized

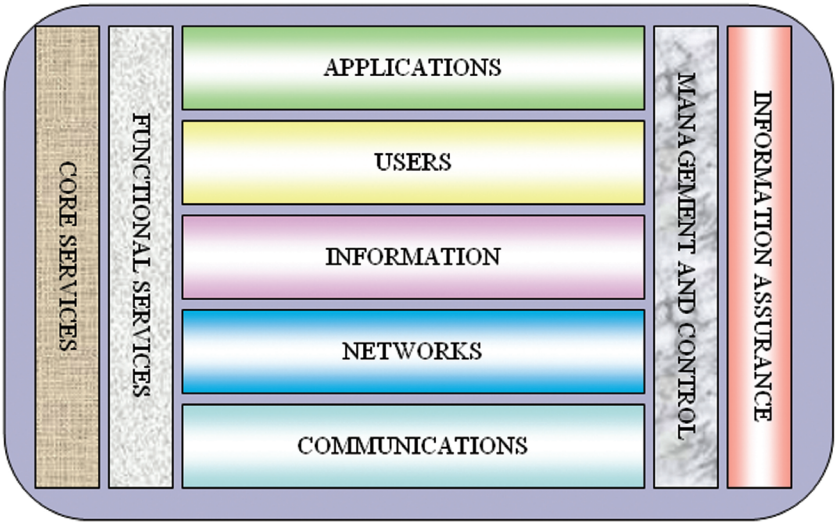

Fig. 2. - *Communications and information system for EU-led Crisis Management Operations (system view)*

in teams of specialized types of communications and information services. Deployable units will organize the operational al helpdesks at headquarters level for assistance, having included in their structure specialists in communications, computing, information assurance and security.

From a system view a crisis management CIS structure can be represented schematically as in **Figure 2** and includes a set of integrated subsystems with the central hub as the communities of interest / users with each individual profile determined by its position in the crisis management system, the right of access to information circulated and the place to access the system.

The principles underlying the design of such a system are: availability, sustainability, reliability, security, flexibility, interoperability and standardization. All subsystems shown in the figure will provide basic services tailored to the needs of the mission and function. The need to extend the services provided in places of permanent locations of communications and information systems, both at institutional and national level will be considered.

Functional and core services provided by a CIS in support of crisis management operations should be planned depending on the nature and extent of the mission, information exchange requirements for command, control, intelligence, surveillance and reconnaissance, the need for cooperation in operational theatre and the location of the field headquarters.

These services can be valuable, based on a robust architecture built on open standards or commercial and private military standards, as appropriate.

Also, services must be correlated in function to the capabilities using ISTAR (Intelligence, Surveillance, Target Acquisition and Reconnaissance) in the mission.

CIS core services of the CIS in support of the EU-led Crisis Management Operations are, as follows:

a) core network services: Common data exchange services, virtualization services, Geo/GIS services, automatic data processing services (office), network search services (web browsing), multimedia (voice, fax, video conferencing) services, import/ export data;

b) services for data interoperability: database replication, military organizational messaging, formatted messaging, e-mail, directory services, storage services, file services, file transfer, multi-service collaboration;

c) security services: authentication, information separation, intrusion detection, integrity services, encryption services, recovery services;

d) services for configuration management: configuration control, network management, data management, central services, security management;

e) communications services: bandwidth management, operational status monitoring, quality of service (QoS), routing services and allocation of streams, IP services,

ISDN services (Integrated Services Digital Network), radio and radio relay services.

Functional services provided by a communications and information system for crisis management could be: joint systems, land forces CIS, air forces CIS, naval forces CIS, logistics CIS, intelligence CIS, special forces CIS and others.

Based on the functional analysis (Timofte G, Tudose E., Vişan D: 2006, p.154) of a general CIS for crisis management the following functions can be identified:

a) The user interface contains all the elements involved in the human-computer interface: phones, fax machines, radios, portable terminals and fixed communications and information systems, screens and keyboards, automatic data conversion devices (scanner) and printers; microphones, speakers, cameras and video monitors system for audio and video teleconferencing and loudspeaker system notification / public announcement.

b) Conference facilities for audio and video teleconferencing secure and non-secure. Teleconferences IP (Internet Protocol) are done through a gateway function, having the role of IP addresses administration and to provide access to security areas defined in the local area network. Services provided under the facility of the conference are: voice / video classified and unclassified, switching and point to point capability and integration of data applications.

c) Area radio coverage provides communications between fixed and mobile units (military or civilian structures, vehicles or individuals) using fixed or portable devices. An implicit requirement of this function is the short message service (SMS). The EU specificity in this area is the radio devices diversity used by the EU military and civilian forces on the ground, on one hand and the need for coordination with all NGOs acting in the same area of operation, on the other hand. Another element of difficulty lies in the lack of coordination between the specialised authority for spectrum management of the EU mission and similar elements on the host nation territory, either because of legislative gap in this field or because of organizational limitations, as the case in many countries on the African continent. An effective spectrum management can be achieved only if the specialized structure of the crisis management mission will take over the responsibility of coordination and allocation of the frequencies for all actors on the operational theatre.

d) Strategic CIS extension. After installing the HQ command post in the theatre, the function modules are connected to CIS for crisis management at tactical level and if necessary with the extensions through modules developed at strategic level. The CIS modules to provide this function should be installed nearby the deployable communication modules that interconnect, the major C2 centers (operational and force

HQs, components HQs, Point of debarkation/ embarkation, etc.).

e) Information Assurance has to support the expansion of the core services and the access to functional applications of the strategic communications and information systems, based on the EU security policy and must also provide a platform for implementing the classified and unclassified domains of the mission. The Information Assurance function should include specialized management function which provides specific information exchange in security field between different systems.

f) Local area Network transport function is provided for interconnecting local area network physical elements of the HQ CIS, ensuring transparent connectivity for all services (packet and circuit switching, access services and local and external functional applications, etc.).

g) Dispersed user interface implements a service interface that can be used to access external networks with packet switching. Access to a network requires the use of an encryption equipment EU accredited to the classified ISDN or IP access router. This function does not replace the LAN infrastructure, but requires that an efficient access solution for staff liaison with the operational headquarters of the mission is implemented. The scenario implementation of this function requires additional protection measures to eliminate or reduce the risk of information compromise, where the user would be forced to facilitate the diversion of any service.

h) The interface function between systems or between different security domains in the same system is achieved through the implementation of the IEG (Information Exchange Gateway).

i) Network management function provides support for the use and maintenance of C2 means, including monitoring tools, configuration, fault detection and isolation, restoration of services on affected components and functions. Management of the deployable CIS provides classified data transport function for traffic management and therefore its separation from the user for all areas of security. For this purpose the encryption protocols and applications management solutions used in conjunction with IPsec will be implemented. Optionally, this function can be implemented in the communications modules and peripherals.

j) The interconnection function ensures interoperability between products, components, modules and systems.

The variety of the theoretical approaches to determine the CIS infrastructure for EU-led civilian and military crisis management operations and missions brings the conclusion that the planning and implementation process is extremely complex, especially in the context of the new security environment. This process requires national participation and adaptation of the national and

institutional development programs in the CIS field. On a short term, one solution could be the extension of the EU institutional operational network, EU OPS WAN, from political-military level in Brussels to the national military representatives in Belgium, and the EU Member States's capitals. This network could be further used for planning, deployment and redeployment of EU forces on missions and operations.

REFERENCES

[1] Burlacu M. (2007) *Operational Headquarter's C4I system for command and control of joint military operations*, PhD thesis, Defence National University "Carol I", Bucharest, p.156.

[2] Timofte G, Tudose E., Vişan D. (2006) *Battlefield digital military communications systems*, Inedit, Bucharest, pp. 70, 154.

[3] Burlacu M. (2005) *C4I systems of modern armed forces of NATO members states. Direction and perspectives on their evolution at the beginning of the 3rd millennium,* scientific research essay, "Carol I" Defence National University, Bucharest, pp. 26-28.

TRENDS IN THE CONVERGENCE OF WIRELESS NETWORKS

Daniel SORA

The Regional Department of Defense Resources Management Studies, Brasov, Romania

In today's technological market, there are many types of networks. These networks include wireless personal area networks (WPANs), wireless local area networks (WLANs), wireless metropolitan area networks (WMANs), and cellular networks. A vision of a future convergence of networks envisaged for WPANs, WLANs, WiMax, and cellular networks is presented in this paper.

Key words: *wireless, networks, convergence, standards, mobile, interoperability.*

1. INTRODUCTION

In today's technological market, there are many types of networks. These networks include wireless personal area networks (WPANs), wireless local area networks (WLANs), wireless metropolitan area networks (WMANs), and cellular networks.

In general, the range coverage of WPANs is smaller than that of WLANs, and that of WLANs is smaller than that of cellular networks. Between WMANs and cellular, their range coverage depends on the frequency band in which they are operating. In each type of network, there are also different categories of networks. For example, there are ZigBee, Bluetooth, WiMedia, and IEEE 8022.15.3c networks in WPANs.

IEEE 802.11 WLANs can be further classified as IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, and draft IEEE 802.11n. These WLANs differ in the data rates that they can deliver. Worldwide interoperability for microwave access (WiMax) is an example of WMAN. On the other hand, cellular networks can be divided into different generations. The first generation (1G) cellular networks are mostly no longer in use. A commonly used second-generation (2G) cellular network today is the global system for mobile communications (GSM). An enhancement of the GSM is the 2.5G general packet radio service (GPRS) cellular network. A third-

generation (3G) cellular network in universal telecommunications systems (UMTSs) is the wideband code-division multiple access (WCDMA) network. Enhancement of the WCDMA is the 3.5G high-speed packet access (HSPA). In North America, there are 2G IS-95 cellular networks and 3G CDMA2000 cellular systems. Another cellular network being standardized is the 3.9G long-term evolution (LTE).

Each of these networks is designed to deliver specific services. These services cannot be migrated to other types of networks. However, there are some bodies that address the needs whereby services can roam from one network to another network based on the best connection available. For example, a local area network (LAN) may be the best connection to the Internet in a fixed office environment. However, a WLAN may be a better option when users need to move from their office to a meeting room. If a user needs to be out of the office most of the time and is often "on the go," he or she may stay connected through a mobile phone or personal digital assistant (PDA). Thus, it would be very convenient for a user if the services she is using can be continued in any environment, whether she is in the office, a meeting room, or out of the office. The mobile device should have a multi-radio that automatically connects the user to the best available network without loss of the service's session during vertical handoff and without intervention. Vertical handoff is the handling of connection from one network to another network that supports a different transmission rate. Thus, interworking is needed between different access networks. A few of these bodies that address the interworking mechanisms are the third-generation partnership project (3GPP), IEEE 802.11u, and IEEE 802.21. 3GPP evolved from the GSM and GPRS cellular networks.

IEEE 802.21 introduces a 2.5 layer between the second and third layers in the OSI/ISO model. The 2.5 layer introduces the media-independent handoff. The aim of this standard is to enable seamless handoff and interoperability between heterogeneous network types, which include both IEEE 802 and non-IEEE 802 networks.

2. 3. GPP/WLAN INTERWORKING

In this form of interworking [1], 3GPP refers to the third-generation partnership project, which evolved from 2G GSM and 2.5G GPRS cellular system; WLAN refers to IEEE 802.11a/b/g wireless local area

networks. Both cellular systems and WLANs are widely deployed in the world today. To provide a seamless experience for a mobile device, interworking mechanisms between cellular systems and WLANs are needed to provide smooth vertical handoff in more complex interworking scenarios.

3. IEEE 802.11u INTERWORKING WITH EXTERNAL NETWORKS

The IEEE 802.11u standard is currently under standardization. The aim of this standard is to amend IEEE 802.11 to add features that will improve interworking with external networks. The interworking between IEEE 802.11 WLAN and external networks is achieved through medium access control (MAC) enhancements.

IEEE 802.11u addresses such areas as enrollment, network selection, emergency call support, user traffic segmentation, and service advertisement.

4. LAN/WLAN/WIMAX/3G INTERWORKING BASED ON IEEE 802.21 MEDIA-INDEPENDENT HANDOFF

The IEEE 802.21 standard is being standardized. The aim of this standard is to enable seamless handoff and interoperability between heterogeneous network types. These heterogeneous network types include both IEEE 802 networks and non–IEEE 802 networks. The IEEE 802 networks are the IEEE 802.3 local area network (LAN), IEEE 802.11 wireless LAN (WLAN), and IEEE 802.16 wireless metropolitan area network (WMAN). The LAN is Ethernet, while the WLAN is Wi-Fi. On the other hand, the WMAN is WiMax. The non-IEEE 802 networks are cellular networks from 3GPP and 3GPP2. 3GPP supports a 3G UMTS, and 3GPP2 supports 3G CDMA2000.

UMTS evolved from 2G GSM and 2.5G GPRS; CDMA2000 evolved from the North America Standard IS-95. The fundamental assumption in the standard is that the mobile devices can support multiple radio interfaces, both wired and wireless, such as Ethernet, Wi-Fi, Bluetooth, WiMax, GSM, GPRS, UMTS, and CDMA2000.

The seamless handoff and inter-operability between heterogeneous network types is achieved by introducing a conceptual layer 2.5. In the traditional OSI/ISO model, layer 1 is the physical layer, and layer 2 is the link layer, consisting of the data link sublayer and the medium access control (MAC)

sublayer. Layer 3 is the network layer. This conceptual layer 2.5 is specified by the media independent handoff (MIH) function. **Figure 1** shows IEEE 802.21 architecture, specifically the interactions between the IEEE 802.21 MIH function and other protocol stack elements.

In IEEE 802.21, one of the main ideas is to provide a common interface for managing events and control messages exchanged between network devices [2]. The outcome of the standard is to provide a general framework applicable from the management and control paradigms of each specific technology and a common interface to the upper layers [2]. These upper layers include the network layer up to the application layer. Besides these functionalities, the standard also introduces an information system (IS) for the storage, management, and communication of system-wide network information [2].

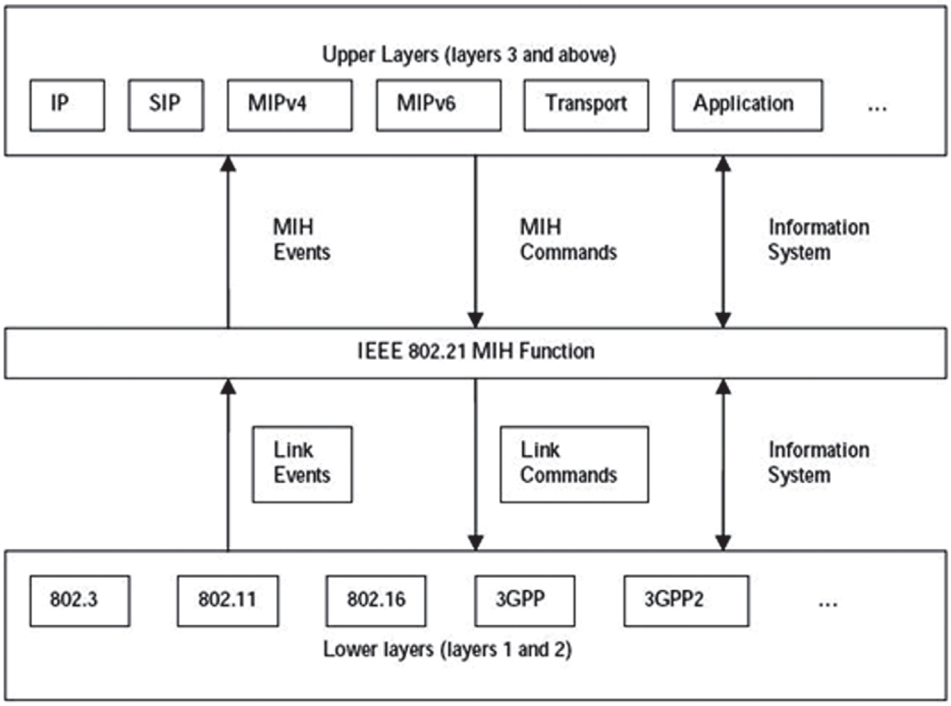

Fig. 1. *IEEE 802.21 architecture*

The IEEE 802.21 MIH function defines three services [3]:

1. Media-independent event service (MIES);
2. Media-independent command service (MICS);
3. Media-independent information service (MIIS).

The MIES provides services to the upper layers of a mobile device by notifying both local and remote events [3]. Local events occur within the local stack of the mobile device, while remote events occur in the IEEE 802.21 MIH function of another mobile device in the network. The event is based on a subscription and notification procedure. The upper layer protocols (layer 3 and above) register a certain set of events to the lower layers (layers 1 and 2) through the IEEE 802.21 MIH function, and they will be notified as these events take place [3]. Information on local events is passed from the lower layers to the higher layers through the IEEE 802.21 MIH function. Information on remote events can be passed to and from the IEEE 802.21 MIH function or layer 3 (L3) mobility protocol in a remote stack. Some common events that are provided by the IEEE 802.21 MIH function are as follows:

- Link up
- Link down
- Link parameters change
- Link going down
- Layer 2 (L2) handoff imminent

The MICS provides primitives to the higher layers to control the functions of the lower layers [3]. MICS commands are used to gather information about the status of the connected links. These commands are also used to execute higher layer mobility and connectivity decisions to the lower layers. Furthermore, these commands can be local and remote. Moreover, these commands can be from the higher layers to the IEEE 802.21 MIH function or from the IEEE 802.21 MIH function to the lower layers. Some examples of these commands that are incorporated in the IEEE 802.21 MIH function are as follows:

- MIH poll
- MIH scan
- MIH configure
- MIH switch

These commands instruct an IEEE 802.21 MIH mobile device to poll connected links to learn their up-to-date status, to scan for newly discovered links, to configure new links, and to switch between available links [3].

The MIIS defines information elements and corresponding query-response mechanisms. These elements and mechanisms allow the IEEE 802.21 MIH function to

discover and obtain information and distribute within a geographical area network information relating to nearby networks [2,3]. The role of MIIS is to provide as much information as possible to the mobile devices on the networks available and the services that they can provide [2]. Furthermore, the MIIS provides the link to access information that is helpful to handoff decisions [3]:

- Network type
- Roaming partners
- Service providers of the neighboring networks
- Channel information
- MAC addresses
- Security information
- Other information on the higher layers.

This information can be made available through the upper and lower layers. The MIIS uses a standard, platform-independent description language to represent the information [2]. External markup language (XML) and type length value (TLV) are two such examples. The information gathered by MIIS can be static or dynamic [2].

Examples of static information are the names and providers of the mobile device's neighboring network; examples of dynamic information are the information on the channel, the security, and the MAC addresses. In some scenarios, some layer 2 information may not be available, or not enough is available to make intelligent handoff decisions. In these cases, upper layers' services may be needed to help in making the decision.

There are two advantages of MIIS: that the information it provides can help significantly in the definition of high-level handoff decisions and policies [2], and that specific access-dependent discovery methods for automatic detection of neighboring networks are avoided.

The IEEE 802.21 standard does not specify rules or policies for handoff decisions and does not dictate that the handoff be a network or mobile-controlled handoff [4].

Concrete rules and policies are beyond the scope of the IEEE 802.21 standard, and their definition and specification are up to the wireless service provider [4].

5. FUTURE CELLULAR/ WIMAX/ WLAN/WPAN INTERWORKING

3GPP is considering cellular networks and WLANs interworking, while IEEE 802.21 is considering a media-independent handoff between LAN, WLAN,WiMax in IEEE, and cellular networks in 3GPP and 3GPP2. We envisage that other technologies for WPANs, such as

Zigbee, Bluetooth, and WiMedia, will also be integrated together with LAN, WLANs, WiMax, GSM, GPRS, UMTS, IS-95, CDMA2000, HSPA, and LTE cellular networks, as shown in Figure 2.

ZigBee is a WPAN that targets applications that require a low data rate, long battery life, and secure networking. ZigBee uses IEEE 802.15.4 specifications. Bluetooth, which is also a WPAN, is used to connect such devices as mobile phones, computers, digital cameras, videogame consoles, and printers over a secure short range unlicensed band. WiMedia is also a WPAN but can support a much higher data rate, up to 480 Mbps. The IEEE 802.15.3c draft and ECMA TC 48 mm Wave draft both operate in the 60-GHz range, and both use directional medium access control (MAC). The IEEE 802.15.3c draft MAC is an extension of the IEEE 802.15.3 MAC, and the ECMA TC 48 mm Wave draft MAC is an extension of the WiMedia ECMA-368 MAC.

IEEE 802.11 is a commonly used WLAN. IEEE 802.11b supports a data rate of up to 11 Mbps, while IEEE 802.11a and IEEE 802.11g support a data rate of up to 54 Mbps. The IEEE 802.11n draft standard supports a data rate of up to 600 Mbps.

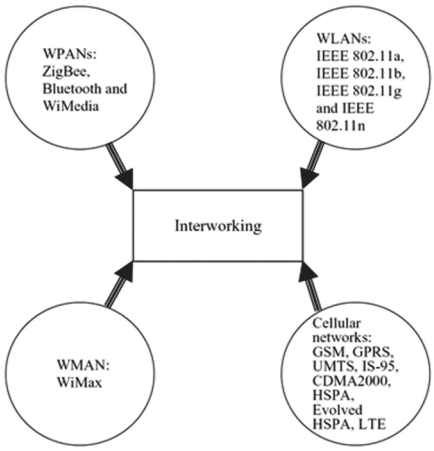

Fig. 2. *Future cellular/WiMax/WLAN/WPAN interworking*

WiMax is a WMAN based on IEEE 802.16. It is used as a last-mile wireless broadband access alternative to cable and digital subscriber line (DSL).

GSM is a second-generation (2G) cellular network; GPRS is a 2.5G cellular network. UMTS is a third-generation (3G) cellular network that uses wideband code-division multiple access (WCDMA) as the multiple-access technology. IS-95 is a 2G code-division multiple access (CDMA)–based cellular network, and CDMA2000 is a 2.5G/3G CDMA standard. HPSA is a 3.5G cellular network designed on top of WCDMA. LTE is a 3.9G cellular network.

The convergence of networks will give rise to many technical challenges. Some of these challenges

include quality-of-service issues, traffic class mappings among different access technologies, vertical handoff mechanisms between access technologies, protocol stack designs, AAA, service discovery mechanism, and routing. Issues in 3GPP/WLAN interworking and IEEE 802.21 media-independent handoff will certainly arise in the convergence of networks that is envisaged.

One of the fundamental factors in the access technologies is data rate. **Table 1** shows the data rates for various access technologies. Due to the different data rates in the access technologies, some services may be terminated during vertical handoffs between access technologies. Rate-adaptive services are also needed when services move from one access technology to another.

Table 1. Data rates for various access technologies

Access Technology	Data Rate
ZigBee	Up to 250 kbps
Bluetooth	Up to 1 Mbps
WiMedia	Up to 480 Mbps
802.15.3c	Up to 6 or 7.35 Gbps
ECMA TC48 mmWave	Up to 6.478 Gbps
WLAN	
802.11b	Up to 11 Mbps
802.11a	Up to 54 Mbps
802.11g	Up to 54 Mbps
802.11n	Up to 600 Mbps
GSM	Up to 9.6 kbps
IS-95	Up to 9.6 kbps (mandatory support)
GPRS	Up to 117 kbps
UMTS	Up to 2 Mbps
CDMA2000	Up to 2 Mbps
WiMax (fixed broadband wireless access)	In excess of 120 Mbps
HSPA	Up to 14.4 Mbps downlink/5.76 Mbps uplink
Evolved HSPA	Up to 42 Mbps downlink
LTE	Up to 100 Mbps downlink/50 Mbps uplink

Mappings of traffic classes between access technologies are dependent on the traffic classes available in each technology. ZigBee has two traffic classes: one based on a contention period (CP), the other based on a contention-free period (CFP) or guaranteed time slot (GTS). The former is based on CSMA/CA and is for non-realtime traffic; the latter is based on reservation and is for real-time traffic. Bluetooth can support voice and data traffic based on polling. WiMedia has four access categories in its prioritized channel access (PCA) mode, and real-time traffic can use its distributed reservation protocol (DRP) mode. The four access categories in PCA are background, best effort, video, and voice traffic. Similarly, IEEE 802.11e EDCA has four traffic access categories: background, best effort, video, and voice. WiMedia PCA is derived from IEEE 802.11e EDCA. Cellular networks 2G and above can support at least voice and data. UMTS can support four traffic classes: background, interactive, streaming, and conversational. WiMax can support at least four scheduling services: best effort, non-real-time polling, real-time polling, and unsolicited grant. Thus, it may not be possible to have one-to-one mapping of traffic classes across all the access technologies.

The types of handoffs in different access technologies are also different. IEEE 802.11 WLAN uses hard handoff; that is, a connection is broken before a new connection is made: break before make handoff. GSM and GPRS cellular networks also use hard handoff, while 2G and 3G CDMA-based cellular networks such as IS-95, CDMA2000, and WCDMA in UMTS use soft handoff. A new connection is made before breaking the old connection in soft handoff, also known as make before break. On the other hand, LTE cellular network uses hard handoff. Thus, different horizontal handoff within each type of access technologies will make the design of vertical handoff between heterogeneous networks challenging.

New protocol stack design such as IEEE 802.21 media-independent handoff will certainly help to alleviate the vertical handoff issues. IEEE 802.21 media-independent handoff should be expanded to include access technologies that are not being considered at the moment as well as future access technologies.

New AAA scenarios also need to be studied to address security, charging, and access. Different access technologies also have different security procedures before a mobile device is granted access. The security architecture and

protocol in IEEE 802.11 is called wired equivalent privacy (WEP). WEP is responsible for providing authentication, confidentiality, and data integrity. Authentication is the process of verifying that a mobile station or user requesting access is, in fact, a legitimate user.

Confidentiality is achieved by sharing a secret key on how to encrypt and decrypt messages. The secret key is the method or algorithm or cipher that the mobile station and the access point use to decrypt messages. Integrity ensures that the message sent by the source to the destination has not been modified or tampered with. GSM uses a 128-bit preshared secret key for securing the interface between the mobile device and the base station. This key is also stored in the authentication center (AuC), which is a database that stores the secret keys of all subscribers. The secret key stored in the SIM card of the mobile device and the AuC forms the foundation for securing the GSM access interface.

GPRS uses the wireless application protocol (WAP). WAP is an open specification that offers a standard method to access Internet-based services and contents. An end-to-end security is achieved by wireless transport layer security (WTLS) in the WAP stack. There is also no key establishment in UMTS. UMTS also uses a 128-bit preshared secret key between the USIM card of the mobile device and the AuC.

Bluetooth uses a large number of keys in its security process. The key hierarchy depends on whether it is unicast or broadcast communication. WiMedia uses a four-way handshaking procedure for two devices to establish pairwise temporal keys (PTKs) and a secure relationship [5]. A device may solicit or distribute group temporal keys (GTKs) within a secure relationship [5]. The security mechanisms in WiMedia control the security operation of devices by setting appropriate security modes [5]. They allow devices to authenticate each other, to derive PTKs, and to establish secure relationships [5]. They also enable devices to solicit or distribute GTKs within established secure relationships [5].

WiMax supports two encryption standards: data encryption standard 3 (DES3) and advanced encryption standard (AES). Thus, different access technologies use different types of security.

Charging or billing is certainly of paramount importance to both the operator and the mobile user. Any simplification in the bill

would be most welcome by the mobile user. Moreover, the operator may also offer an overall cheaper plan to the subscriber using the heterogeneous networks due to new revenues generated in the new services introduced across the access technologies. Service discovery mechanisms are also needed for a mobile device to discover new services and networks within its region. A mobile device can find more about the available access technologies and their services in its vicinity. These will enable it to connect to the available best connection (ABC).

Effective routing protocols in the WPANs are also needed to support all possible services and their QoS constraints. Enabling services with QoS constraints to be met in multihop WPANs is certainly an important technical challenge.

Many challenging technical issues need to be solved before the convergence of networks envisaged in this section can be realized. However, once it is achieved, mobile users can enjoy the fruits of this labor.

6. SUMMARY

3GPP/WLAN interworking between cellular technologies and WLANs, IEEE 802.11u interworking of IEEE 802.11 WLANs with external networks, and IEEE 802.21 media-independent handoff for heterogeneous access technologies such as IEEE 802.3, IEEE 802.11, IEEE 802.16, 3GPP cellular networks, and 3GPP2 cellular networks are certainly the specifications and standards to look for in the convergence of networks today.

The future envisaged for cellular/WiMax/WLAN/WPAN interworking in a convergence of networks, and some issues relating to the interworkings of various access technologies, are discussed in this chapter. Once these interworkings between technologies are achieved, together with new rate adaptive services across them, users can enjoy truly seamless and user-transparent connectivity based on the best connection available.

REFERENCES

[1] *** (2007) *"3rd Generation Partnership Project: technical specification group services and system aspects; feasibility study on 3GPP system to wireless local area network (WLAN) internetworking,* (Release 7)", 3GPP TR 22.934 V7.0.0.

[2] F. Cacace and L. Vollero. (2006) *"Managing mobility and adaptation in upcoming 82.21-enabled devices,"* WMASH 2006, Los Angeles, CA, Sept. 29.

[3] A. Dutta, S. Das, D. Famolari, Y. Ohba, K. Taniuchi, V. Fajardi, R. M. Lopez, T. Kodama, and H. Schulzrinne, (2007) *"Seamless proactive handoff across heterogeneous access networks",* Wireless Personal Commun., vol. 43, pp. 837–855.

[4] A. de la Olivia, T. Melia, A. Vidal, C. J. Bernardos, I. Soto, and A. Banchs, (2007) *"A case study: IEEE 802.21 enabled mobile terminals for optimized WLAN/3G handovers",* Mobile Comput. Commun. Rev., vol. 11, no. 2, Apr.

[5]*** (2005) *"High rate ultra wideband PHY and MAC standard",* Standard ECMA-368, ECMA International, Geneva, Dec. 2005.

[6] E. Stevens-Navarros, C. Sun, and V. W. S. Wong. (2007) *"A survey of analytical modeling for cellular/WLAN interworking",* in Emerging Technologies in Wireless LANs: Theory, Design and Deployment, Cambridge University Press, New York.

[7] E. Stevens-Navarros and V. W. S. Wong (2007) *"Resource sharing in an integrated wireless cellular/WLAN system",* Canadian Conference on Electrical and Computer Engineering 2007, Vancouver, British Columbia, Canada, Apr.

[8] W. Song, H. Jiang, and W. Zhuang. (2007) *"Performance analysis of the WLAN-first scheme in cellular/WLAN interworking",* IEEE Trans. Wireless Com0mun., vol. 6, no. 5, pp. 1932–1943, May 2007.

[9] W. Song and W. Zhuang, *"Multi-service load sharing for resource management in the cellular/WLAN integrated network,"* IEEE Trans. Wireless Commun.

INTELLIGENCE SHARING AND DISSEMINATION IN COMBINED JOINT SPECIAL OPERATIONS

Florin NEGULESCU

Special Operations Forces Battalion, Romania

The vast majority of military strategists agree with the importance of intelligence as a decisive factor during the planning and execution of successful military operations. The intelligence process consists of five phases: Planning and Direction, Collection, Processing and Exploatation, Analysis and Production, and Dissemination and Integration. All these stages are of equal importance in the effort to provide intelligence in support of military operations. However, most analyses concerning the modernization of procedures and technologies required to improve the intelligence process mainly focus on the collection phase of the intelligence cycle. Perhaps the most disadvantaged phase of the intelligence process, in terms of methodological progress, is the intelligence dissemination phase. The purpose of this article is to stress the importance of the intelligence dissemination phase of the intelligence process and to identify the difficulties encountered in this phase during the planning and execution of CJSO (Combined Joint Special Operations).

Key words: *intelligence, intelligence sharing, Combined Joint Special Operations, planning, execution.*

> *"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle".*
>
> Sun Tzu

1. INTRODUCTION

The vast majority of military strategists agree with the importance of intelligence as a decisive factor during the planning and execution of successful military operations. As shown below in Figure 1, the intelligence process consists of five phases: Planning and Direction, Collection, Processing and Exploatation, Analysis and Production, and Dissemination and integration (DoD, 2007, p. I-7).

All these stages are of equal importance in the effort to provide intelligence in support of military operations. However, most analyses concerning the modernization of procedures and technologies required to improve the intelligence process mainly focus on the collection phase of the intelligence cycle. Perhaps the most disadvantaged phase of the intelligence process, in terms of methodological progress, is the intelligence dissemination phase.

Fig.1. *The Intelligence Process (From DoD, 2007, p. I-7) 14*

The purpose of this article is to stress the importance of the intelligence dissemination phase of the intelligence process and to identify the difficulties encountered in this phase during the planning and execution of CJSO (Combined Joint Special Operations).

2. THE IMPORTANCE OF INTELLIGENCE SHARING AND DISSEMINATION

No matter how well planned and targeted the intelligence collection effort is, it becomes inefficient if the means and methods of collecting information are inadequate, insufficient or obsolete. Regardless of how much qualitative information is collected, it loses much of its value if it is not properly processed. No matter how well processed the collected information is, it can become a double-edged sword either if it is not properly analyzed, or if the analysis is not transformed into finite and qualitative intelligence products. More importantly, even if all four of the phases above have been successfully carried out, the whole intelligence process will be for naught if the final products of the intelligence process do not reach the final users. To fail during the dissemination phase of the intelligence process means, in fact, to miss the purpose of the entire intelligence cycle (DeConde, 2002, pp. 225-226).

The risk of failure during the intelligence dissemination phase may be emphasized by one psychological element in the intelligence analyst's way of thinking. Once the pressure during the information collection and analysis has passed, and the intelligence products are completed, the intelligence analysts may have a tendency to partially lose their focus, which may affect the intelligence dissemination phase (Maltz & Kohli, 1995).

Moreover, the information/ intelligence sharing among various elements of a Combined Joint Special Operations Task Force — which is actually a more difficult case of intelligence dissemination — affects the intelligence process starting with the collection phase. Vanotten (2005) observed that, "anytime people from different cultures come into contact

with one another, there is the potential for tension and misunderstanding" (p. 32). He suggested that a psychological premise might slow down the information/intelligence sharing process. Such a premise may arise because of differences between the intelligence cultures of the CJSOTF (Combined Joint Special Operations Task Force) members. Moreover, it may arise because, at times, some CJSOTF members might consider themselves superior to the other members.

The processes of intelligence dissemination and intelligence sharing, which are quite similar from the methodological point of view, are extremely important, interoperable elements of a military coalition (Neagoe, 2009:25).Therefore, intelligence dissemination must be treated with the same attention as any other phase of the intelligence process.

3. INTELLIGENCE IN COMBINED JOINT SPECIAL OPERATIONS

Perhaps the most complex environment in which information/ intelligence is disseminated and shared is the combined joint environment. The globalization of threats requires the globalization of efforts to eliminate these threats. CJSO represent one of the ways in which militaries respond to these threats.

CJSO are characterized by a few elements that differentiate them from traditional military operations. In essence, the CJSO involve the joint action of two or more special services, belonging to two or more states, in order to eliminate a threat to the security of those states (DoD, 2008, p. 108). In terms of intelligence, the following features characterize the CJSO environment:

- Different intelligence cultures, from country to country;
- Different intelligence cultures, from service to service;
- Differences between special operations forces' intelligence requirements and conventional forces' intelligence requirements;
- Different systems, technologies, methods and regulations used by the CJSOTF members during the intelligence process;
- Differing individual country security issues.

4. ISSUES IN INTELLIGENCE SHARING AND DISSEMINATION DURING COMBINED JOINT SPECIAL OPERATIONS

Traditionally, Special Operations may be classified into two main categories: commando type and unconventional type (Lamb, 1995, p. 4). CJSO are not an exception to th is general classification.

1. Commando Type - Combined Joint Special Operations

Commando type operations are characterized by high physical risk for the performers in the field, high

political risk for the planners, short execution time and high strategic stakes for the operations. In terms of intelligence dissemination and sharing during the CJSO, there are a number of issues that may reduce the efficiency of the intelligence cycle.

These problems may arise even from the beginning of the planning process due to the high strategic stakes of these operations, which sometimes involve highly sensitive intelligence held by one or more of the states engaged in operations. In this respect, the suspicions and hesitations of some countries to share intelligence - sometimes because of the higher price for which the intelligence has been obtained, or the desire to protect the country's sources - have become the main elements that slow down the process of intelligence dissemination and sharing during the CJSO.

Moreover, because the available time to prepare the commando type-CJSO is limited, it is difficult to build an efficient intelligence architecture that is able to facilitate the intelligence sharing and dissemination (Walsh, 2007, pp. 151-181).

Another limitation in terms of intelligence sharing and dissemination is sometimes represented by the high degree of the information's sensitivity. Sometimes this situation limits the access to certain information for the particular members of the CJSOTF.

An example of how information sensitivity affects the intelligence sharing process exists when special operation forces are involved in the execution of a mission with conventional forces, or when NATO states are involved in the execution of a mission with non-NATO states.

In the latter case, NATO members may have access to some sensitive information but, due to the information's degree of confidentiality, the members cannot disclose this information to nonNATO states.

2. Unconventional Type - Combined Joint Special Operations

Since the commando type-CJSO are usually short operations, unconventional type-CJSO are long duration operations. Because of their protracted character, the volume of information is typically very large in unconventional type-CJSO.

In their study focused on the general dissemination of market intelligence, professors Maltz and Kohli (1996) discovered that the receiver's perception of the quality of the intelligence might be diminished by a very large amount of information. Moreover, they found that *"if new information is transmitted at a rate that goes above the receiver's capability to process it, the receiver might perceive the information to be uncertain, incomplete, or contradictory"* (pp. 49-50).

There is no reason to assume that in the case of military intelligence the situation would be different. This circumstance calls for the creation of an intelligence infrastructure with a complex and flexible architecture capable of dealing with a huge volume of information. Although a

technical infrastructure is essential to facilitate the intelligence sharing and dissemination process, paradoxically this infrastructure may sometimes alter the process (Office of the Director of National Intelligence, 2008, pp. 3-4).

This situation may arise due to the following reasons:

- the need for an accommodation period for the new staff to learn operating rules and characteristics of the technological infrastructure and the intelligence architecture;
- the existence of an enormous intelligence database not managed well enough through efficient software;
- the lack of technical and operational knowledge necessary to work with the intelligence for some CJSOTF's staff personnel.

5. CONCLUSIONS

In combined joint operations, each allied nation has, more or less, a different set of regulations regarding intelligence sharing and dissemination. This situation affects the CJSO and requires that a method to coordinate and harmonize these regulations be found.

Recently, referring to coalition operations in Afghanistan, Maj. Gen. Gratien Maire (2008), the French embassy's defense attaché in Washington, highlighted the necessity to find a solution for this issue. Military officials must *"find the way either to adapt the regulations or to find a way to make sure that because of a regulation, we would not be in a situation where some commander in the field will not be able to provide some intelligence for the troops that could perhaps save lives"*, he stated.

The issues in sharing and disseminating intelligence within CJSO cannot be solved by a universal formula. The intelligence sharing and dissemination process' optimization can be achieved on a case-by-case basis by using different methods. However, a few general conclusions can be highlighted in order to guide this optimization process by focusing the efforts on the following areas:

- the creation of an intelligence architecture capable of providing effective and well-defined channels through which to achieve the intelligence sharing and dissemination;
- the implementation of simple and efficient standard reporting procedures;
- the creation of a proficient Combined Joint Intelligence Team capable of managing the intelligence flux during the short or protracted combined joint special operations;
- the use of simple and efficient software for intelligence management in order to facilitate the categorization and dissemination of intelligence;
- the establishment of a clear policy regarding the sharing and dissemination of classified information.

Moreover, Lowenthal (2006) identified the following questions

that must be taken into consideration during the intelligence dissemination phase of intelligence cycle:

- Among the large mass of material being collected and analyzed each day, what is important enough to report?
- To which policy makers should it be reported - the most senior or lower-ranking ones? To many, or just a few?
- How quickly should it be reported? Is it urgent enough to require immediate delivery, or can it wait for one of the reports that senior policy makers receive the next morning?
- How much detail should be reported to the various intelligence consumers? How long should the report be?
- What is the best vehicle for reporting it-one of the items in the product line, a memo, a briefing (pp. 63-64)?

Those questions are applicable for the intelligence dissemination phase of the CJSOTF's intelligence cycle as well.

REFERENCES

[1] Department of Defense. (2007). Joint Publication 2-0., Joint Intelligence. Retrieved October 15, 2008, from http://www.dtic.mil/doctrine/jel/new_pubs/jp2_0.pdf

[2] DeConde, A. (2002). Encyclopedia of American Foreign Policy, Second Edition, Volume 2, New York : Scribner.

[3] Department of Defense. (2008, October 17). Joint Publication 1-02., DOD Dictionary of Military and Associated Terms. Retrieved October 25, 2008 from http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf.

[4] Lamb, C. (1995). Perspectives on Emerging SOF Roles and Missions. Retrieved November 2, 2008 from http://www.soc.mil/swcs/swmag/9507.pdf.

[5] Lowenthal, M. (2005). Intelligence, From Secrets to Policy. (Third Edition) Washington, DC: CQ Press.

[6] Maire, G. (2008). Regulations problematic, Inside the Pentagon. Retrieved December 25, 2008, from http://www.insidedefense.com.libproxy.nps.edu/secure/display.asp?docnum=PENTAGON-24-39-8&f=defense_2002.ask.

[7] Maltz, E.,& Kohli, A. K. (1996). Market Intelligence Dissemination Across Functional Boundaries. (Journal of Marketing Research-February, 33, 47-61). Retrieved December 18, 2008 from http://www.jstor.org/stable/3152012

[8] Neagoe, V. (2009). 185 days in Irak. Bucharest: Editura Militara

[9] Office of the Director of National Intelligence. (2008). Intelligence Community Information Sharing Strategy. Retrieved January 16, 2009 from http://www.dni.gov/reports/IC_Information_Sharing_Strategy.pdf

[10] VanOtten, A. G. (2005, January-March). Culture Matters. (Military Intelligence Professional Bulletin, 31, 1). Retrieved December 21, 2008 from http://www.fas.org/irp/agency/army/mipb/2005_01.pdf.

[11] Walsh, I. J. (2007). Defection and Hierarchy in International Intelligence Sharing.(Journal of Public Policy, Vol. 27; Part 2, pages 151-182). London: Cambridge University Press.

HUMAN SECURITY: CONSEQUENCE OF AND INCENTIVE FOR NATIONAL AND INTERNATIONAL SECURITY

Florentin Adrian ILIE

Military lawyer, Parliament Liaison and Legal Assistance Directorate,
Ministry of National Defense, Bucharest, Romania

In the evolution framework of modern society conflicts, even though not of a global outreach, have unprececedently increased in number and effects. As a result, human security, has become of top concern in democratic states. In order to understand this trend and as a result of the importance acquiered by the the concept of "human security", it is important to undertake an investigation into its dimensions and variables. Thus, the assumption underlying this article is that human security is both a consequence and an incentive for the national and international security.

Key words: *human security, economic security, food security, environment security, personal security, community and political security.*

At the moment, both specialized literature and the external policies of some states offer a a plethora of definitions related to the concept of human security.

Thus, one such definition belongs to Kofi Annan, the seventh UN General Secretary between 1997-2006, and is included in the "Millenium Report" [1]. According to him, due to contemporary conflicts, the concept of security has evolved. If in the past, it was synonymous with territorial defense against external attacks, because of current security imperatives, the concept has also come to refer to community and people's protection against state domestic violence. The necessity of a more people centered approach to security is argued by threats such as the weapons of mass destruction and, more specifically, nuclear weapons.

The same former UN representative emphasized the complex relationship established between the concepts of peace and security. Thus, to him, peace is more than the absence of war. On the other hand, human security can no longer be understood strictly form a military point of view. Thus, human security also refers to economic development, social justice, environmental protection, democratization, disarmament and respect for human rights and state sovereignty.

Other opinions of importance for the proper understanding of the concept of human security belong to Sadako Ogata, former United Nations High Commissioner for Refugees, Government of Canada, and UN Development Program and underline two aspects of human security. First, the concept refers to ensuring security against chronic threats such as famine, diseases and repression. Second, it refers to identifying the right means to protect people against the sudden and painful disruption of their daily work and life patterns [2].

Authors such as Kanti Bajpai [3], Anne Hammerstad [4], Gary King and Christopher Murray [5] take a broader view on the concept. Thus, they believe that, regardless of the approach taken to security (*i.e.* critical or human), the latter's aim is to ensure the social, political, economic and environmental conditions needed for a free and dignified life.

In our opinion, human security must be viewed in accordance with the provisions of legal principles in the field and is the result of the relationship established between human rights and the obligation of international actors to respect them. The human rights we are referring to here are the fundamental ones that any human is entitled to. As for the states and international organizations it is within their power and responsibility to ensure the necessary framework for the exercise of human rights.

Based on the above definitions, it is obvious that human security is a global issue, of concern to the people from both poor and developed countries. Thus, many of the current threats, such as human rights violation, organized crime, drugs, pollution, unemployment, are common to all countries. Even though their intensity differs from country to country, on overall, they are real, continuously evolving and interconnected. Thus, when human security is at risk somewhere in the world, all nations may be affected. Famine, epidemics, pollution, drug trafficking, terrorism, ethnic tensions, social disintegration are no longer isolated events, limited national borders since their consequences can spread out at regional or global level. It is easier and less costly to ensure human security through prevention measures rather than through intervention mechanisms subsequent to security disruption. Therefore, human security is about an individual's level of integration into society, about the level of freedom in exercising the right of choosing among alternatives, as well as about the responsibility on behalf of international establishments acting in the filed of human rights to ensure all of the above.

The UN Development program provides a long list of threats to human security out of which the following are important to highlight: economic security, food security, health, environment security, personal security, community and political security.

Economic security refers to the entitlement of any individual to

have a minimum regular income that comes from a lucrative activity or, as a last resort, from a social security trust fund. Taking such a view can only mean that only a quarter of the whole world' population benefits from economic security. Even if the problems related to economic insecurity are greater in the developing countries, the developed states also show concern for these. In this respect, unemployment is considered one of the factors that lead to political tensions and interethnic violence.

Food security refers to the economic and physical possibility of all people to meet their basic food needs. According to a UN report, it is not the presence of food that raises problems, but the deficiencies in food distribution and the absence of the financial means to purchase it.

Health security guarantees people's basic protection against diseases and an unhealthy lifestyle. In the developing countries, the main causes of death are infectious diseases that kill approximately 17 million people a year. On the other hand, in industrialized states the highest number of health problems is related to the circulatory system, about 5.5. million people dying every year on account of that.

According to the United Nations, both in industrialized countries and in developing countries the threats to health security are greater in the case of the poor people, mostly children, from rural areas. The most common problems of these are malnutrition, lack of drinkable water and insufficient medical services.

Environmental security refers to people's protection against natural disasters, as well as against the continuous deterioration of the environment. In developing countries, the main environmental threat is the absence of access to clean water. At the same time, in developed countries, atmospheric pollution is the main cause of concern. Moreover, global warming caused by the greenhouse effect is another major environmental threat to human security.

The goal of ensuring personal security is to protect individuals against physical violence inflicted upon them by another state, by their own state or by violent people.

Community security aims at preventing the decay and loss of traditional human relationships and community values. In this respect, the most endangered communities are those of the minority ethnic groups.

Finally, political security is about the extent to which individuals live in a society in which human rights are observed [6]. Thus, huma right violation is more likely to occur in times of political instability.

The rich and often painful experience in the field of human security has led to the identification of unequivocal instruments that can be grouped into:

- UN instruments, such as the UN Charter, the Universal Declaration of Human Rights, the Pact On Political and Civil Rights;

- instruments of the Council of Europe, namely the Convention on Human Rights, The (reviewed) European Social Chart;
- EU instruments like the Lisbon Treaty, the Security Strategy;
- NATO instruments: the NATO Treaty and the Strategic Concepts of 1991, 1999, and 2010.

Due to their complexity, the accomplishment of human security objectives has often required resorting to means of high impact in the military field. Thus, the efforts to achieve human security are not only economic or political by nature, but military as well.

In this respect, peacekeeping operations, humanitarian interventions, demining actions, mass destruction weapons removal are some of the military instruments aimed at increasing the human security level.

Some of the main roles [7] played by the military forces in the protection and insurance of human security are as follows: protection of human life during war and observance of the Geneva Conventions and of international norms in order to keep the number of civil casualties to a minimum and to allow the access of humanitarian actors into theatres of operations.

The "occupying" actor is responsible for insuring the fundamental security and welfare prerequisites for the civil population. In this respect, protection is a fundamental role on behalf of the military forces in order to prevent manslaughter. According to the principles set out by the International Commission for Intervention and State Sovereignty, peacekeeping missions under UN mandate are organized and conducted in order to prevent large scale violence against civilians. Civilian protection is viewed as one of the goals of peacekeeping operations, even though not listed among the major ones. Thus, the protection role actually consists in securing the area for humanitarian intervention on behalf of international players in charge of supporting civilians. Granting protection is an important component of humanitarian and relief programs and, in this respect, suffices to remind that, for example, the refugee camps are situated in areas where the risk of threats is minimum. The potential role of the military in such circumstances is to reduce threats by a dissuading presence. In this respect, some military analysts argue that civilians could benefit more from a combat force that could stop enemies' actions.

Regardless of the role assumed by the military forces, ensuring human security, even at a basic level, should be part of any military action and not just a minor goal. Thus, observance of international legislation is only one of the ways in which human security can be achieved.

The events occurring for the past decades have made stability operations one of the major means of solving conflicts and of accomplishing human security.

It is common truth that nowadays conflicts are the main menace to human security. As a result, the international community created new instruments to ensure and maintain long lasting peace.

From this point of view there are four aspects of the military intervention that shoud be reminded and they are as follows:

- The intervention should not be viewed as an opportunity to use force since the vision and the commitment to maintain peace, as well as the humanitarian assistance and reconstruction efforts vary by region.
- The traditional concept of sovereignty is not an obstacle to taking action in humanitarian crises. In this respect, the way states view the concept of national interest is very important since a new definition of it is necessary. Thus, nowadays, the states make joint efforts towards achieving common goals and maintaining common values and therefore, national interest actually becomes collective interest.
- If intervention by force is necessary the UN Security Council must be able to meet the inherent challenges. Moreover, when fighting stops the commitment for peace of the international community should be as strong as during wartime.

The UN Charter acknowledges the legal status of the human rights included in the Universal Declaration of Human Rights. Achieving equilibrium between the political and the humanitarian issues difficult, and the relationship between the military and civil actors concerned with accomplishing humanitarian goals is fragile but very important. If such issues are not carefully managed, humanitarian interventions can lead to human casualties, can cause even more problems if not deepen the existing ones that they are supposed to solve.

The subject of human security is a complex one and cannot be fully covered in one journal article. However, it is obvious that if humans and their security are not of primary cconcern in contemporary society, than all its accomplishments lose their importance and diminish their value. Therefore, in future research endeavors we will focus more on the less analyzed aspects of the concept of human security and we will try to highlight the benefits of placing the individual at the core of the national and international efforts directed towards the protection and insurance of security.

REFERENCES

[1] *** (2000) Millenium Report of the Secretary General, United Nations, Chapter 3, pp.43-44, last retrieved from http://www.un.org/millennium/sg/report/full.htm on 08/22/01.

[2] *** (1994) United Nations Development Programme (UNDP). Human Development Report 1994. New York: Oxford University Press, p. 23.

[3] Kanti Bajpai. The Idea of a Human Security Audit. Joan B. Kroc Institute Report, No. 19. Fall 2000, p. 1-4. last retrieved from http://www.nd.edu/~krocinst/ocpapers/op_19_1.PDF on 08/22/01.

[4] Anne Hammerstad (2000) Whose Security? UNHCR, Refugee Protection and State Security After the Cold War, Security Dialogue 31.4 (2000): 395.

[5] Gary King and Christopher Murray. "Rethinking Human Security." Political Science Quarterly. (Winter 2002): In Press. Manuscript, p. 2. last retrieved from http://gking.harvard.edu/files/hs.pdf on 08/22/01.

[6] according to a study conducted by Amnesty International, political repression, systematic torture and bad treatment are still being practiced in 110 counties in the world.

[7] Holt, Victoria K., The military and civilian protection: developing roles and capacities, HPG Research Briefing, No. 22, March 2006, p. 2, apud Homan, Kees, The military and human security, în „Security and Human Rights", No.1/2008, p. 74.

[8] *** United Nations Charter.

[9] *** NATO Treaty.

[10] *** The Social European Charter (reviewed).

[11] *** The European Convention on Human Rights.

[12] *** The Pact on Political and Civil Rights.

[13] *** NATO Summit - Washington, 3-4 April, 1999.

[14] NATO Summit - Prague, 21-22 November, 2002.

[15] *** NATO Summit - Istanbul, 28-29 June, 2004.

[16] *** NATO Summit - Riga, 28-29 November, 2006.

[17] *** NATO Summit - Bucharest, 2-4 April, 2008.

[18] *** NATO Summit - Strasbourg, France/ Kehl, Germany, 3-4 April, 2009.

[19] *** NATO Summit – Lisbon, 19-20 November, 2010.

INFORMATION ASSURANCE-INTELLIGENCE-INFORMATION SUPERIORITY RELATIONSHIP WITHIN NATO OPERATIONS

COL. (ret) Professor, Ph.D., Gheorghe BOARU*
LTC Ioan-Mihai ILIEŞ**

*"CAROL I" National Defense University, Bucharest, Romania
**HUMINT Center of Excellence, Oradea, Romania

There is a tight relationship between information assurance, the intelligence cycle and information superiority within NATO operations. The intelligence cycle has a discrete architecture and provides on-time and relevant intelligence products to the joint force commanders and to other authorized users in a specific joint area of operations. The intelligence cycle must follow the evolution of the operation. A permanent intelligence estimate will be performed during the military decision making process and operations execution. Information superiority is one of the most powerful intelligence cycle achievements. and decisively infuences the success of NATO joint operations. Information superiority must be preserved and enhanced through information assurance. Information assurance is an information operation that must be planned by the military in charge of operation security or by non-military experts, executed by all personnel during the entire intelligence cycle life time and employed during the planning and execution of NATO joint operations.

Key words: *NATO, information, information assurance, intelligence, information superiority.*

1. INTRODUCTION

The aim of this article is to provide a brief theoretical overview of the relationship between information assurance-intelligence-information superiority and thus enhance the existing knowledge about the preparation and execution of operations in a multinational environment. As a result of the research conducted in this field the article is structured in two main parts. The first one provides a comparative terminological analysis of the following terms "security of information", "information security (INFOSEC)" and "information assurance". The references used for this part are the NATO Security Directive, the experience gained in this field by the U.S. Army and by the Romanian Army, and the practices of some international players and non-military personnel working in the area of information security. The second part focuses on the role and principles

of intelligence within NATO, as well as on the relationships between data, information and intelligence at NATO level by highlighting the role of information assurance in achieving and maintaining information superiority in North Atlantic Treaty Organization. Depending on the views expressed in the doctrines, manuals, courses, studies or papers consulted for this article, the authors take the liberty to express their agreement or disagreement on the issues under discussion.

At a bird's eye view, the various international and national military directives and handbooks in the fields of information, information security and information assurance, intelligence and information superiority consulted for this article talk about similar concepts by different names. This is all too natural since a military theory is continuously evolving depending on the transformations lying ahead. Thus, the meanings associated to the aforementioned terms have varied in time and they still do depending on the contexts in which they are used. In this respect, it is worth reminding that Romania's status of NATO member does not rule out the necessity to make full meaning of the concepts currently employed in operations.

Another important conclusion issuing upon the consultation of various provisions of NATO, the U.S. and Romanian battlefield handbooks concerning concepts related to operating systems/functions of fighting in general and operating system/fighting function in particular is that no clear cut parallelism is to be drawn among these. Thus, one should emphasize the fact that for reasons such as mentality, level of technical training and fighting equipment not all the provisions of NATO and American handbooks can indiscriminately be applied to the Romanian military doctrines.

Even though from a theoretical standpoint one can state that there are no marked differences in concepts usage between the Romanian military and its allies, at a practical level the differences are more than obvious. For example, in their intelligence doctrines, allies like the USA, United Kingdom, Germany provide the right amount of detail in accordance with the type of work to be done. Moreover, when focusing on the field manuals of these state militaries, any researcher can conclude that the latter not ony mirror the doctrines, the terms and concepts related to operational language but also clearly present and explain them with no redundant terminology, no interpretations, no unnecessary additions.

By comparison, Romanian provisions related to some of the basic aspects concerning the decision making process (including information security or information assurance) are approached from different perspectives depending on the Romanian handbooks presenting

them. Thus, commanders often find themselves in an uncomfortable position when they have to make a summary of the basic aspects to be taken into account when making decisions, a summary that is vital in achieving the desired end-state, namely inclusion in the higher echelon commander's intention and executing the mission received from the latter. Such a situation is to be understood simply because, at present, the Standing Operating Procedure (SOP) drawn up by the military staffs, especially the chapter on information/intelligence, is a solution adopted by the Romanian commanders out of necessity.

Therefore, the authors of the article emphasize the clear cut difference that must be made from the onset between the terms of information and intelligence. Moreover, when analyzing these, one should also take into account the following relationship: data -information - (products) intelligence - relevant information - execution information, a relationship already detailed in other papers of this article's authors. In this respect, mention should be made of a landmark document issued in 2005, namely the Romanian Army Doctrine for Information, that plays a major role in making clear delineations among often confused and misused concepts and terms, some of which will also be presented in this paper. Thus, one final aim of this paper is to provide better knowledge of NATO operations mechanism by focusing on some elements, phenomena, and processes in accordance with the relationship between information security and information superiority.

2. SECURITY OF INFORMATION - INFORMATION SECURITY (INFOSEC)-INFORMATION ASSURANCE: A TERMINOLOGICAL OVERVIEW

Within NATO operations there is a distinct relationship between the nominal phrases: security of information, information security and information assurance. The first term, security of information, refers to information in general, in other words, security of all types of information. Moreover, the same phrase encompasses the term of information security (INFOSEC) since the latter means security of information handled in electronic systems. In other words, one can say that INFOSEC is security of electronic information. Moreover, both these terms are part of the information assurance term, the latter referring to information systems security in general.

However, "information systems" is a comprehensive term that includes all the aspects related to infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information.

As far as the relationship between data – information – information assurance – intelligence and the comparison betwen the process of data transformation into knowledge and the understanding of intelligence as a warfighting function, one can underline three distinct aspects.

First, intelligence is a very important process for the military decision making process (MDMP) during the preparation and execution of NATO operations. The intelligence process has a cycle which includes four phases: direction, collection, processing and disemination of intelligence products to the commanders, staffs and other users. In addition, two more phases are permanently performed, namely the evaluation and the feedback.

Second, intelligence is an important warfighting function that provides allied comanders with an important instrument that allows for the use of the combat power of their military structures at the right moment and in the right place.

Third, information assurance is vital for the intelligence cycle and must be performed in order to assure the disemination of the intelligence products only to authorized personnel and in an extremely secure mode.

Upon the thorough analysis of the information assurance and intelligence processes within NATO operations, the authors of this article can only conclude that the main effort of the Allied Operations is initially focused on intelligence, information assurance and logistics. For mission execution, commanders need early development of a secured intelligence architecture in Theatre of Operations. That means deployable information security personnel and resources, military intelligence forces/structures/groups and a flexible approach to the command and control relationship. Performing the operations objectives requires the Joint Force Commander to determine with his commanders, as soon as possible, the critical information requirements. The intelligence community has to put in place a robust and versatile intelligence network in designated Area of Operations. The security structures must perform complex information assurance operations for intelligence cycle protection.

However, information assurance determines all information flows within the specific information systems, while security of information ensures protective measures of all types of information in general, providing the Confidentiality, Integrity and Availability (CIA) for all-source-information.

For a clearer understanding of security of information and for achieving a very good level of security for classified information a clear access authorization must be established. Security classification is of utmost importance for information protection and applied to information

to indicate the possible damage to the security of NATO and/or its member nations if the information is subjected to unauthorized disclosure. The security structure should maintain a list indicating the levels of access for each assigned individual who is granted access to NATO information and should verify NATO access authorizations for all personnel. In our opinion, as with classified information, access is not based on duty position, rank, or level of clearance. Access is based on need-to-know, the proper level of clearance, and an access briefing for a specific level and type of classified information.

Within NATO, there are many concerns over security assurance. In our opinion, these concerns that are very clearly expressed by the allied military analysts are related to the strategic dilemma of nowadays global information environment, namely the desire to exploit the Computer Network Operations advantage as opposed to the protection of the global information environment. In order to solve the dilemma, those working in the military have to focus on the lessons learned in the field.

Thus, after the 9/11 events, one can discuss about another kind of war, the war against terrorism that invoves anti-terrorist and counter-terrorist actions. The terrorist attacks are not only by bombs and arms. Therefore, taking into account that contemporary society is an information society based on computer networks, in the war against terrorism a very important confrontation is the cyber one. Cyber confrontation means cyber attack and cyber defense. In our opinion, the cyber terrorist actions are cyber attacks and not only the reactive but also the proactive actions are cyber defence.

All this considered, the question for the Romanian military, but also for all those working in the field approched by this article should ask themselves if they and/the state is prepared in case of a terrorist attack. The terrorists have sufficient means and determination to perform cyber attacks. Moreover, the question should also focus on whether people are prepared for a cyber terrorist attack. In our opinion, managing to clarify the inherent concepts associated to these may ensure the winning of a battle in the field.

One of the biggest potential threats to information security is the people who operate the computers. A workplace may have excellent information security systems in place, but security can be easily compromised. If a help desk worker gives out or resets passwords without verifying who the information is for, then anyone can easily gain access to the system. Computer operators should be made fully aware of the importance of security. Simple security measures can be used by everyone to keep data secure. For example, changing passwords on

computers, and using combinations of letters and numbers makes it harder for hackers to gain access. Also, a note of passwords is not to be made where it can be easily accessed. However, there has never been such a thing as a totally secure system. Hackers will always find more sophisticated ways to gain access. However, with technology implementing higher levels of information security, such as iris recognition systems, security systems should keep us out for a little longer.

In conclusion, there is a distinct relationship between security of information, information security and information assurance, as already highlighted in this part of the article.

3. THE RELATIONSHIP BETWEEN INFORMATION ASSURANCE AND INFORMATION SUPERIORITY

As pointed out in the introduction, the research already conducted in the field of information security manageemnt yielded another relationship that is worth analyzing and clarifying, namely the one between information assurance and information superiority. Thus, one has to emphasize the tight and discrete relationship between data, information, information assurance, and intelligence within NATO. Intelligence is not only the product resulting from the intelligence cycle but also intelligence generate through the intelligence warfighting function. Intelligence staffs direct collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations.

The approach taken towards the analysis of information and information threats and to the explanation of the information assurance role in obtaining and preserving the information superiority within the NATO operations resembles that of NATO military operations Thus, the key words of this part of the article are: NATO, information, intelligence role and cycle, information assurance and information superiority. Moreover, the information assurance role in the data - information - intelligence relationship must also be underlined. In this respect, when analyzing this relationship one can easily observe that when the intelligence cycle is performed the information assurance for it is fundamental. In other words, information must be protected during the intelligence process. The intelligence products have to be made available for authorized users in a very secure mode. Thus, even though data and information collection and evaluation processes can be by the book, clear estimations and interpretations can be achieved, excellent conclusions

can be presented to commanders, if a very strong system for security of information is not in place, all of the above are in vain. In this respect, it is the the breaches and gaps in the security of information systems that enemies always look for. Therefore, good information assurance is the basic element in information protection. More than that, in our opinion, information assurance is an information operation that protects and defends information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. In other words, information assurance is a very important information operation performed to protect information systems.

Thus, the need for information assurance within the information operations conducted by the Alliance must be emphasized. Moreover, the cue for a real understanding of the role played by information assurance in NATO forces achieving information superiority in theaters of operations lies in the explanation of the relationship between information security, intelligence cycle in NATO operations, and the role of information security to achieve and maintain information superiority in NATO.

Accordingly, the intelligence cycle is defined as a discrete transformation of data and information into intelligence products. The intelligence cycle phases overlap and coincide, so that they are concurrent and continuous rather than sequential. The intelligence cycle decisively directs the military commanders' decision-making process and operation execution. The intelligence products have to be predictive and support the commander in understanding the common operational picture of his designated operation area. The intelligence products are the result of obtaining relevant information. A permanent intelligence estimate is be performed during the "plan, prepare, execute" operations cycle. Information assurance has the role of protecting all information flows and systems. Information superiority is greatly influenced by the information assurance operation and the intelligence cycle products. The information superiority is decisive and determines the success of the joint operations. It is not only the security personnel who must be involved in the security and information assurance of the NATO operation, but also all the military and non-military personnel deployed in a specific theatre of operations.

The role of information assurance is a basic one in maintaining the information superiority within the national and NATO doctrines. A very short analysis of the relationship between information superiority and

information assurance is absolutely necessary. According to the Romanian doctrine [1], information superiority means the collection, processing and dissemination of an accurate and credible information flow, and denying similar actions of enemy forces. As defined by Romanian military experts [2], information superiority refers to relevant information processed for a comprehensive understanding of the operational environment, enemy actions and intentions, and for generating the common operational picture. Within NATO doctrine [3], information superiority is analyzed as part of the operational concept. Thus, information superiority within allied operations is a very complex process which comprises an information operations strategy established by the designated allied structure inside the Joint Force Command. This allied structure coordinates special operations, intelligence operations, civil-military cooperation (CIMIC) operations, communication and information systems installation, command and control systems, security operations, deception operations, psychological and electronic warfare operations.

Information superiority and air superioriy/supremacy and naval presence before the joint forces engagement in battle are the main aspects of a successful combined joint task force in NATO operations. Information systems and networks provide the predominant source from which the warfighter generates, receives, shares, and utilizes information. The installation of an advanced communications and information system which is able to sustain the dissemination of products through a certain intelligence cycle

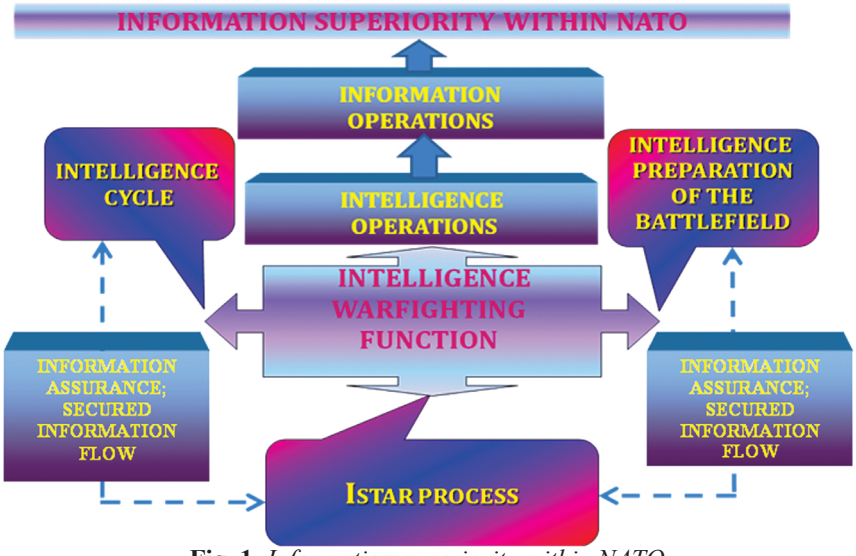

Fig. 1. *Information superiority within NATO*

(properly applied during the military decision making-process), leads to information superiority, which is essential to achieving success in all military operations.

The power of superiority in the information environment mandates the joint force commanders to fight for it as a first priority even before hostilities begin. The quality of information depends upon the accuracy, timeliness, relevance, usability, and completeness of information from all sources. A top responsibility of command is to ensure access to all relevant information sources within and among all military and non-military organizations which are involved in joint military operations or non-military operations (according to NATO comprehensive approach), and in multinational operations with mission partners. The continuous sharing of information from a variety of sources facilitates joint force mission execution in a specific area of operation and timelineness awareness for multinational military and non-military structures.

In conclusion, information superiority cannot be achieved without information operations, namely without information assurance operations. The security quality criteria of the information must be assured and preserved by the entire personnel during a NATO operation. In this respect, it is worth reminding the the new NATO concept: "need to know vs. need to share" and the two approaches to this subject. Thus, while the former refers to the intelligence products which need to be shared to partners in an area of operation, the latter is about the necessity to know how to share information by applying all the security measures needed when transferring information. Otherwise, the Wiki leaks lessons learned can repeat.

Last but not the least, the importance of information assurance for the intelligence cycle and for information superiority within NATO operations must be emphasized. The intelligence provides on time and relevant intelligence products to the joint force commanders and other authorized users in a specific joint area of operations. The intelligence cycle must follow the evolution of the operation. A permanent intelligence estimate is performed during the military decision-making process and operations execution. Information superiority is one of the most powerful intelligence cycle achievements and decisively infuences the success of joint operations. Information superiority must be preserved and enhanced through information assurance. Information assurance is an information operation that must be planned by the military staff and executed by the entire personnel during the entire intelligence cycle life time.

4. ACKNOWLEDGEMENT

The information in this paper is public or unclassified. Some of the ideas presented in the article were discussed during the postgraduate course in Information Security Management attended in 2011 at the Regional Department of Defense Resources Management Studies, Braşov. Moreover, the opinions already expressed are the result of consulting an extensive bibliography as part of the PhD research project of LTC Ioan-Mihai ILIEŞ undertaken at "CAROL" I National Defense University of Bucharest, Romania under the supervision and guidance of COL (ret) Professor, Ph.D., Gheorghe BOARU.

REFERENCES

[1] Information support of Joint Operations, (Bucharest, 2003), 58.

[2] Constantin Alexandrescu, Gelu Alexandrescu and Gheorghe Boaru, Military Information Systems, (Bucharest: National Defence University "Carol I", 2010), 25.

[3] AJP-03, Allied Joint Operations, (2002), 2-22, 4-13.

THE IDENTITY PERSPECTIVE WITHIN THE INTERCULTURAL RELATIONSHIPS ESTABLISHED IN THEATERS OF OPERATIONS

Adrian LESENCIUC

Faculty of Aeronautical Management, "Henri Coanda"
Air Force Academy, Brasov, Romania

Identity, a self-defining feature in relation with others, represents one of the standpoints when studying intercultural relationships within the theatres of operations. Military personnel participating in different missions in these theatres are characterized by markers of ascribed identity. The Romanian military personnel participating in international missions cannot be only characterized by their ethnic identity as long as one's identity is multiple and reflects the relationship(s) established with various social and professional groups. Unfortunately, despite the depreciation of the ascribed identity role in comparison with the optional identity role, transnational organizations do not represent a landmark for the identity of Romanians in general, and of Romanian military, in particular. Moreover, the optional identity contributes to alienation and self-closing, and not to the strengthening of relations with the military group assumed to be the group of belonging.

Key words: *cultures, identity, intercultural relationships, theatres of operations, group*

1. INTRODUCTION. THE CULTURAL IDENTITY ISSUE

The issue of cultural identity takes into account the possibility of cultural configuration/reconfiguration. In an attempt to outline different definitions of culture, starting with those identified by Kroeber and Kluckhohn (1954/1978) and continuing with the classification of these definitions by different cultural categories included in Jencks' studies (1993:7-24), Margareta Boacă (2009:63) notices that the general outlook on culture is that of a social category. This aspect is relevant in terms of achieving the intercultural standpoint between individuals and distinct communities within the theatres of operations and in terms of switching from "culture" (the singular form), as a term defining a general reality, to *"cultures"* (the plural form), a term that reflects the specificity, uniqueness and coherence of each cultural space. This perspective, also called in terms that are more restrictive "the social perspective", represents the basis of our investigation in the substantiation

of the necessary instruments that come from distinct disciplinary areas like sociology, anthropology or social studies and is not a limitative one. On the contrary, it represents a way of highlighting the links between disciplines belonging to wider fields, in a manner similar to the interdisciplinary alliance prefigured by Cicourel (apud Mattelart & Mattelart, 2004:115). Within this wide and fluctuant disciplinary field, and within the specific domain of our research, namely intercultural communication, the issue of switching from culture (the singular form) to cultures (the plural form) becomes relevant. In the context of the actual cross-cultural dynamics and of the trends to abandon the physical boundaries of the social framework, as in the case of the theaters of operations, the mentioned issue becomes more relevant.

The identity issue has deep roots. Even if in the contemporary context identity is understood as a mark of profound transformations in society, the individual dimension of identity must not be abandoned. This dimension represents the ground that feeds the entire construct of identity. Identity designates a substitutable characteristic of persons (or objects, phenomena, events, statements) in real or projected plan (Larousse, 2006:554). Moreover, identity consists in the manner in which one defines as himself (Mathews, apud Boacă, 2009:128). This perspective is deeply rooted in the Hegelian conception of identity revelation regarding the antithetical relation with the other that leads to self-identification by resorting to the absolute self-consciousness as a landmark. The persons' identity could take at least one of the forms: the biological identity, the belonging of the individual to the human species; the psychological identity, highlighted by the hereditary inheritance, bearing the mark of the family; and the socio-cultural identity, defined by the elements that determine the specificity of the social and cultural frame to which an individual belongs.

2. THE CULTURAL IDENTITY ISSUE WITHIN THE THEATRES OF OPERATIONS

From the perspective of the factors that determine the nature of intercultural relationships established during the peacekeeping operations, the third dimension (the socio-cultural) is the one that represents the defining frame of identity. This dimension is conditioned by the biological and psychological dimensions of identity; therefore, the approach should aim the inter-dimensional interpretation, not the separation required by the deconstructivist approach. The pluri- and trans-dimensional brings into question the Freudian perspective, in accordance with which the need of identity defines the man. The way of development is narcissistic. Under the pressure of Eros and Thanatos the ego as a psychical instance, the manager of identity in the contact with the exterior is, in the end, perceived as itself.

"Moreover, this identity becomes object of transaction and imitation; identity is "borrowed" in a superior stage of imitation, i.e. of similar answering reaction from the exterior, comparative with an observed pattern. This transaction of identity becomes a manner of social learning and involves more than simple imitation: the contagiousness, which is the basis of the group identity formation. In this manner, the birth culture marks our identity. The specific genetic dowry and the access to education represent the prerequisites for the development of human identity. The same processes take place in the construction of individual and collective identity". (Lesenciuc *et al.*, 2010:134-135).

The necessary differentiation that needs to be done when it comes to identity delineation, respectively emphasizing the aggressiveness/ hostility in the process of configuring the identity, thrusts into the limelight the intergroup, racial and national differences as explained through the libido concept (Freud, 1951:37-38). The latter highlights the narcissistic attitude of groups characterized by the preoccupation for self and native and by the rejection of the allogeneic (especially when the Others' attitudes contradict the narcissistic opinion about self). The perception is not determined by the identification of common elements, but it is marked by differences, even if the "Cain and Abel syndrome" is present (*i.e.* if the probability of hostility is high in the conditions in which the differences between groups are low, then the relationship is closer (apud Boacă, 2009:129)). In this respect, we can take into account the third dimension of identity, the socio-cultural one, which leads to group formation and, implicitly, to group identity. Freud analyzes the factors suggested by Le Bon in relation with the the fear of isolation and the contagiousness, all of which are seen as easy to be established, but hard to explain: "they must be included among those phenomena of a hypnotic order" (Freud, 1951:10).

From the perspective of the reports drawn up during the peacekeeping operations, the complex problem of identity is related to the fact that the identity matrix is built within a cultural framework. As such, the cultural borders are enforced through certain differentiating elements - markers of identity- that are inherited: the language, the nationality, the religion, a certain social class, certain communication patterns, diverse habits and norms that regulate everyday life. These characteristics that imply minimum control and enough conscientious influence concerning each of the individuals could not be overridden by our behavior or by our own Weltanschauung. This form of identity that is as a mark of culture contains characteristics that are less under control. However, it targets the set of adequate interpretation, confers a form of identity designated by Giddens (1991:105) through the phrase "ascribed identity".

When approaching the identity issue during peacekeeping operations in relation with the group (military group, in this case) one can observe

a twofold tendency: on one hand, a differentiation and fragmentation process that characterizes the relationship between the group and its outsiders/exterior, and on the other hand a process of self-organization. Therefore, we conclude that, in defining his own identity, the individual within the group is exposed to different pressures that come from the relationship to be established with different identities on various levels. Whatever the predominant or the reference level is, the differences in perception lead to shaping and highlighting the particularities that are often under the influence of the type of relationship experienced with the exterior in terms of cultural identity forming. Let us notice that individual identity does not imply a clear limit, a state in a particular frame reported to others, a relation with a specific group, but it involves a series of successive and relative stages between the individual identity and the anthropological identity of the species. One of these intermediary stages is the ethnical stage, ethnicity being the natural and legitimate state of each nation. National identity can therefore be seen as an intermediary stage in a pattern of identities which includes, as its limits, the individual identity and the species identity. In this case, the problem of national identity is the one that will have the strongest impact in indentifying the factors which determine the nature of intercultural relations established within the theatres of operations.

National identity, approached in the context of cultural and political identities' superposition, represents a synthesis of cultural, social, political, and economic features accomplished through the comprehension/ internalization of the set of cultural and common moral values. Such a synthesis can be compared to the unfastened links between tangible entities (individuals) on one hand, and between tangible entities (individuals) and abstract entities (the nation) on the other hand.

3. ROMANIAN IDENTITY. CHALLENGES CHARACTERISTIC OF THEATRES OF OPERATIONS

The Romanian ethno-type has its basis on a common symbolical heritage, but a heritage which has set apart the engagement in politics and the reflection upon its role and meaning. This orientation, which apparently is one towards the interior, towards the one's self, stems from the unfastened link with space and not with time. As a result, it provides the Romanian individual with a set of successive closings understood as the consolidation of his own system of values, or more precisely as "closings within opening" (Noica) and involving the enrichment of Being, defined by means of the encompassing adverb "homely" and through the extension towards new spaces translated holographically into one's own being. "Home/homely" triggers cultural identity and its meaning is derived from Havel's concentric closings intents: from the planetary level (the species' identity) to the individual level (the ego's level), that is the core

around which the proximity of the birthplace, of the region, of the country entwines (apud Brumaru, 2001:194-195). These circles, these meanings of "home/homely" and the inherent stages of the identity as described by Georgiu (Georgiu, 1997:77) represent the object of our study. Thereby, the national identity problem, as an intermediary stage in the Havel-Georgiu structure of defining elements and brought up into discussion is only one cultural facet.

The cultural problem resulting from the cooperation/competition relations between different nations' representatives dates back much further than the establishment dates of global (transnational) organizations such as UN, ECSO, NATO, EU, etc. Therefore, we cannot assess it by only referring to such organizations. The issue of national/cultural identity in transnational organizations is identical to the issue of strengthening the role of society within community. Thus, such a simile reveals an obvious tendency to ignore ethnical identity, to diminish the role of a group's identity in favor of personal identity. In 1990 Stuart Hall noted: *"There are no natural links which bind humans together; people are responsible for their own bonds, craftsmen of their own connections"* (Hall, 1990:228). From this point of view, cultural identity is no longer an assigned/pre-established identity, but a matter of personal choice, and thus based on elements chosen by the individual in accordance with his predilections and personal options. As a result, in an era when all cultural resources are available, the risks for of an individual to make random choices or to resort to the "cultural" products insistently offered by the media are omnipresent and that is a direct consequence of the absence of a frame of reference and system of values. The ever increasing number of possible choices to be made leads only to despair in front of countless options. This kind of identity is temporary, perishable, fragile, because it has no basis, no durability, no appreciation.

4. CONCLUSIONS

The presence of the Romanian officers in peacekeeping operations should be analyzed from the identity perspective suggested by this article. Thus, they are both representatives of the Romanian society, of their own communities, and of the international organizations coordinating the activity within the theatres of operations. As such, they are from the very beginning "fighters" for their own cultural identity. Such a perspective on identity leads us to Young's statement underlining that *"just as community collapses, identity is invented "* (apud Bauman, 2001:11) and which points out the following paradoxes: the community paradox and the identity paradox. These two are actually the ones that come at play and have a say in the positions assumed by any Romanian officer deployed in theatres of operations. Mention should be made that the Romanian officer's ethno-psychological profile is not substantially different from the Romanian ethno-type given the

differences that are more of nuance than of essence. As such, entering a swirling movement, this officer is expected to choose (often intuitively) the middle way between acting as a community representative characterized by a certain cultural identity, or as the representative of society characterized by a personal "mark". Furthermore, under the protection of this fragile balance, throughout a volatile area of operations, he must put the efficient communication card on the table. Intercultural communication, which must be institutionally developed in terms of competence, has the role of diminishing the perception, representation and projection disequilibrium, but also the role of providing a certain opening, facilitating relationship development and collaboration, allowing for the tuning of social mechanisms, for the growth of collective solidarity, for the reconciliation and the redefinition of identity, etc.

Taking into account the lack of a curriculum on intercultural communication, the aim of our research is to investigate the extent to which the power of communication – a distinctive Romanian feature – occurs in the absence of a common educational framework at national level. Thereby, we conclude that the process of sorting out the factors, which determine the nature of intercultural relationships established during peacekeeping operations, is not limited to an enumeration, but implies the identification of the means by which these factors are activated during the participation of the Romanian officers to peacekeeping operations.

REFERENCES

[1] Bauman, Z. (2001) Comunitatea. Căutarea siguranței într-o lume nesigură. București: Antet.

[2] Boacă, M. (2009) Comunicarea interculturală în contextul proceselor de integrare europeană și euroatrlantică. Bucharest: "Carol I" National Defense University Publishing House.

[3] Brumaru, A. I. (2001). Despre ființa românească. Bucharest: Viitorul românesc Publishing House.

[4] Freud, S. (1951). Group Psychology and the Analysis of the Ego. New York: Liveright Publishing Corporation.

[5] Georgiu, G. (1997). Națiune, cultură, identitate. Bucharest: Diogene.

[6] Giddens, A. (1991). Modernity and Self-Identity. Self and Society in the Late Modern Age. Stanford: Stanford University Press.

[7] Hall, S. (1990). "Cultural identity and diaspora". In Jonathan RUTHERFORD (ed.). Identity: Community, Culture, Difference. London: Lawrence & Wishart.

[8] Jencks, C. (1993). Culture. Florence: Routledge.

[9] Kroeber, A., Kluckhorn, Clyde. (1954) (1978). Culture: A Critical Review of Concepts and Definitions. New York: Random House.

[10] Lesenciuc, A., Neblea, Alexandra, Radu, Ioana. „Dimensiuni identitare ale studenților militari". In Ioan Deac, Margareta Boacă (eds.). Sesiunea de comunicări științifice „Securitate și apărare europeană în contextul crizei economico-financiare", secțiunea 9, 15-16 aprilie 2010

[11] Mattelart, A., Mattelart, M. [1995] (2004). Theories of communication. A short introduction. Thousand Oaks, CA: SAGE Publications Inc.

[12] *** (2006). Larousse. Marele dicționar al psihologiei. Bucharest : Trei Publishing House. Bucharest: "Carol I" National Defense University Publishing House.

POLITENESS IN REQUESTS: SOME RESEARCH FINDINGS RELEVANT FOR INTERCULTURAL ENCOUNTERS

Aura CODREANU*
Alina DEBU**

* PhD, MA, MSc, Regional Department of Defense Resources Management Studies, Brasov, Romania;
** MA, Teacher of Romanian language, Fagaras, Romania

The major aim of this article is to analyze the relationship between indirectness and politeness in requests. The research project supporting the findings of the paper was undertaken in order to find out to what extent politeness and indirectness are viewed as overlapping or mutually excluding categories by Romanians compared to other nationalities, such as the British and the Hebrew. Another inherent goal of the paper is to provide an example of the socio linguistics instruments that can be employed in the investigation of the differences and similarities likely to emerge in intercultural encounters. Thus, we believe that only through similar research undertaken in the fields contributing to the emerging field of interculturality one can actually trespass the theoretical assumptions and move on to the identification of the right tools and means through which intercultural discourse to be approached at a pragmatic level and thus better understood and taught in educational establishments.

Key words: *social linguistics, requests, politeness, indirectness, intercultural relationships, interculturality*

1. INTRODUCTION

One of the issues of major concern when it comes to intercultural encounters is the socio linguistic discourse of politeness. Even though at a theoretical and practical level extensive reserch in the field has already been conducted (Leech, 1983: 108, S. Blum-Kulka: 1987, Yong-Ju Rue, Grace Qiao Zhang: 2008, María Elena Placencia: 2007, Carmen Taleghani-Nikazm: 2006), little research has been conducted so far into the politeness discourse of Romanians as compared to other nations. Therefore, we believe that this article may contribute to a research niche neglected so far and, hopefully, provide a theoretical and practical framework for further investigations into the field of polite

requests. Moreover, we would like to emphasize the importance of taking such a specific approach when it comes to understanding intercultural relationships from a socio linguistic perspective. Thus, what generally is viewed as common sense knowledge and hence prone to misunderstandings may become substantiated information and assumptions contributing to a btetter approach to intercultural encounters between Romanians and other nations.

2. THEORETICAL BACKGROUND

Before presenting the research project supporting the aim(s) of this article, our undertaking needs some background to the issue of politeness in requests through indirect strategies. Thus, in the literature on politeness and indirectness, it is often argued that the two notions represent parallel dimensions. For instance, Leech (1983:108) suggests that given the same propositional context, it is possible *"to increase the degree of politeness by using a more and more indirect kind of illocution .Illocutions tend to be more polite because they increase the degree of optionality and because the more indirect an illocution is, the more diminished and tentative its force tends to be"*. On the other hand, S. Blum-Kulka (1987) believes that, at least for requests, such claims as those upheld by Leech, need to be modified by distinguishing between two types of indirectness: conventional and non-conventional, the concept of politeness being associated with the former *"but not necessarily with the latter"* (1987:132) [1]. Further on, from the same study we find out that for S. Blum-Kulka politeness represents the interactional balance achieved between two needs: the need for pragmatic clarity and the need to avoid coerciveness. Thus, this balance seems to be achieved, in Blum-Kulka's opinion, in the case of conventional indirectness.

3. RESEARCH QUESTIONS

Starting from this theoretical background, we tried to find out whether Romanians associate politeness with conventional indirectness, as Blum Kulka asserts, or they consider non-conventional indirectness as more polite. Moreover, we tried to identify if there are any similarities between the answers of the Romanian respondents and those of Blum Kulka's respondents.

4. METHODOLOGY, SURVEY QUESTIONS AND SAMPLE DESCRIPTION

In order to attain these objectives, we used the method called *"the discourse completion test"* (DCT). This method basically consists in creating a certain situation, where respondents are asked to engage in a conversation about a certain ordinary problem. The researcher gives the participants the first part of the conversation along with a description of the situation and asks the informant to complete this situation by supplying a continuation.

The situation designed for our research was as follows:

"You are asked by your teacher to make some reading notes of the last novel you were supposed to read. You come to school next day and realize that you forgot to do that. You need those reading notes, so you try to get them from your colleagues. What do you say?"

The next step we took consisted in providing the respondents a typology of request patterns, listed in **Table 1** [2], a typology that follows the classifications of request strategies on scales of indirectness achieved by Searle (1975), Ervin-Trip (1976), Blum-Kulka (1982). The scale is based on postulating degrees of illocutionary transparency. This means that, the more "indirect" the mode of realization, the higher will be the interpretive demands on the hearer' (1987:133). Thus, the request patterns considered as the most direct or transparent are the ones in which the request's force is either marked syntactically, or indicated explicitly, as in Mood Derivable (1) and Performative (2).The least direct patterns are considered to be those in which requestive force is not indicated by any conventional means and hence has to be inferred, as in Hints (8). Between these two extremes there are patterns that derive their relative transparency either from conventions in the wording of the speech act, such as Hedged Performatives (3), or from conventions regarding the semantic contents which, by social conventions, count as potential requests, such as Obligations (4), Want Statements (5), Suggestory Formulae (6) as well as the group of strategies often referred to in the literature as "conventionally indirect" (Blum-Kulka 1987 apud Searle 1975) referred to in the table as Query Preparatory (7).

Table 1: Eight types of request strategies used in the research

Descriptive category	Example
1. Mood Derivable	Give me your lecture notes.
2. Performative	I'm asking you to give me your notes.
3. Hedged Performative	I would like to ask you to give me your notes.
4. Obligation statement	You'll have to give me your notes
5. Want statement	I would like you to give me your notes.
6. Suggestory Formulae	How about giving me your notes?
7. Query Preparatory	Could you give me your notes?
8. Hints	I didn't take any notes and I don't want to get a bad mark.

This table, along with the situation presented above, was administered to ten people [3] aged between 20- 40. They were asked to rate each utterance on a one to eight point scale for either "directness" or "politeness". Moreover, in order to ensure that judgments of directness and politeness would relate only to these strategy types we avoided both internal and external modifications, such as hedges (*i.e.* "please"), in the case of politeness strategies or justifications in the case of directness. Besides that, as the appendix makes it obvious, the eight utterances were typed randomly.

5. SURVEY FINDINGS

The results were as follow:

Out of the eight utterances four were pointed out as the most preferred, namely those belonging to the query preparatory category (chosen by seven respondents), to the want statement category (by two respondents) and to the hedged performatives and hints by one respondent.

In terms of directness and indirectness, and politeness, the answers provided by the respondents were somewhat similar to the previous choices. Thus, in terms of the categories mentioned above seven respondents came up with the orders below:

Table 2: Directness scale

Strategy type	**Direct**
4. Obligation statement	
6. Suggestory Formulae	
5. Want statement	
3. Hedged Performative	
2.Performative	
7. Query Preparatory	
8. Hints	
3. Hedged Performative	
	Indirect

Table 3: Politeness scale

Strategy type	Most polite
7. Query Preparatory	
3. Hedged Performative	
6. Suggestory Formulae	
8. Hints	
5. Want statement	
1. Mood Derivable	
2. Performative	
4. Obligation statement	
	Least polite

Two other respondents made somewhat different choices presented below:

Table 4: Directness scale

Strategy type	Direct
1. Mood Derivable	
2. Performative	
4. Obligation statement	
6. Suggestory Formulae	
5. Want statement	
3. Hedged Performative	
8. Hints	
7. Query Preparatory	
	Indirect

Table 5: Politeness scale

Strategy type	Most polite
3. Hedged Performative	
7. Query Preparatory	
8. Hints	
6. Suggestory Formulae	
5. Want statement	
4. Obligation statement	
2. Performative	
1. Mood Derivable	
	Least polite

The solutions chosen by one respondent are only partially different from the others' respondents. Thus, the order is the following:

Table 6: Directness scale

Strategy type	Direct
1. Mood Derivable	
2. Performative	
4. Obligation statement	
6. Suggestory Formulae	
7. Query Preparatory	
5. Want statement	
3. Hedged Performative	
8. Hints	
	Indirect

Table 7: Politeness scale

Strategy type	Most polite
8. Hints	
3. Hedged Performative	
5. Want statement	
7. Query Preparatory	
6. Suggestory Formulae	
4. Obligation statement	
2. Performative	
1. Mood Derivable	
	Least polite

6. DATA ANALYSIS

It is worth underlining that only one respondent chose hedged performatives and hints as the answers favored in dealing with the situation given by the researchers correlating them both in terms of the most polite and conventional indirect

categories. Consequently, we will not take these answers into account due to their singularity. However, if the survey is to be carried out on a larger group of respondents it would be interesting to check if there are any other respondents favoring hints and hedged performatives as both the most polite and conventionally indirect strategies to be used in a certain context. If these answers will check out, then Blum Kulka's theory is to be confirmed. However, due to the limits of this research posed by the restricted sample of respondents, as well as by the restrictive situation that contextualizes only certain socio-pragmatic aspects (i.e. relationship between the language and the level of respondents' education, relationships set by the imaginary situation), we will focus on the bulk of the answers and thus ensure the reliability of the research.

A comparison between the answers of the other respondents is made through the **Table no. 8.1.** and **Table no. 8.2.** below and comments are made on the findings.

As it becomes obvious from the two tables, the seven respondents that chose to deal with the situation presented by the survey in terms of query preparatory utterances prove to be constant in their choices by pointing out to the same answer as the most polite and as second in indirectness on the indirect- direct scale. In contrast, the other two respondents, although choosing want statements as the one they would personally use in a specific situation, select as perceiving hedged performatives, query preparatory, hints and sugestory formulae as the most polite while replacing the latter with want statements when it comes to the indirectness scale.

Thus, narrowing the research findings by focusing only on the first four most polite utterances we are left with the following strategy types: Hedged Performative; Query Preparatory; Hints; Suggestory Formulae. Moreover, by contrasting the last four choices for the most indirect strategies, we are left with only three strategies, namely Hedged Performative; Hints; Query Preparatory. Thus, by applying the principle of overlapping categories, we are left with three strategies of conventional indirect politeness: Hedged Performative; Hints; Query Preparatory utterances.

7. RESEARCH CONCLUSIONS

The conclusion to be drawn based on the findings and after the data analysis is that while most respondents (*i.e.* seven) choose the same strategy (*i.e.* query preparatory) as an individual manner of self-expression, as well as a strategy perceived equally polite and indirect, the other two respondents seem to contradict themselves. However, we cannot claim them unreliable because in our view there may be differences between what one person uses on a daily basis and what the same person perceives as adquat, acceptable in terms of polite indirect strategies.

Table 8: Data analysis

8.1. Directness scale

Strategy type/ No. of respondents: 7	Direct	Strategy type/ No. of respondents - 2	Direct
1. Mood Derivable		1. Mood Derivable	
4. Obligation statement		2. Performative	
6. Suggestory Formulae		4. Obligation statement	
5. Want statement		6. Suggestory Formulae	
3. Hedged Performative		5. Want statement	
2. Performative		3. Hedged Performative	
7. Query Prepartory		8. Hints	
8. Hints	Indirect	7. Query Preparatory	Indirect

8.2. Politeness scale

Strategy type/ No. of respondents: 7	More polite	Strategy type/ No. of respondents - 2	Direct
7. Query Preparatory		3. Hedged Performative	
3. Hedged Performative		7. Query Preparatory	
6. Suggestory Formulae		8. Hints	
8. Hints		6. Suggestory Formulae	
5. Want statement		5. Want statement	
1. Mood Derivable		4. Obligation statement	
2. Performative		2. Performative	
4. Obligation statement		1. Mood Derivable	
	Less polite		Indirect

Consequently, the current paper proposes two possible directions of investigation. One of them should be focused on the relationship between what a person believes to be polite in a certain situation and what the same person perceives as polite. Thus, such an investigation should be focused on the differences/ similarities between individual choice on one hand, and societal and linguistic norms as taught in school or within family on the other hand.

The second direction of future research should focus on checking the findings of the current research against a larger group of Romanian respondents. However, based on our findings according to which Hedged Performative; Hints; Query Preparatory utterances we will try in the next paragraphs to draw a comparison with Blum Kulka's findings about the British' and Jews' usage of conventional indirect polite strategies.

8. POLITE REQUESTS IN ROMANIAN, ENGLISH AND HEBREW

In terms of query preparatory utterances in all three languages the latter are viewed as conventional indirect polite strategies and are ranked in the first two positions. However, if Romanians list the same category either on the seventh or the eighth position on the directness scale, for Hebrew the utterances appear on the sixth position, whereas in English they appear on the fifth position. Thus, the conclusion could be that Romanians are more likely to use conventional indirect strategies than other nationalities (at least in terms of perception of what things should be like until further research proves otherwise).

Hedged performatives as polite strategies are ranked second in Hebrew, and first or second in Romanian. Unlike these two languages, English ranks them on the fourth position. Once again, Romanian and Hebrew rank these utterances as to their directness/ indirectness on the sixth position, whereas English on the fifth. This second type of utterances seem to point out to similarities between Hebrew and Romanian, an aspect which is to be researched in detail in the future.

As for the last type of utterances, hints, Romanian overlaps with Hebrew and English in terms of politeness, in all three languages hints being perceived as the most indirect strategies. However, the slight differences between the three languages appear when it comes to politeness. Thus, Romanian places such utterances on the third or fourth position; Hebrew on the fourth or fifth position and English on the second or third position. As it is obvious, in this respect, Romanian seems again to overlap with Hebrew.

If we restrict the categories that are ranked as both the most polite and the most indirect, in Hebrew we are left with Hints, Query Preparatory and Hedged Performatives, whereas in English with Query Preparatory, Hints, Hedged Performatives, Suggestory. Comparing the situation with Romanian, English introduces a category that we left aside in this research since it was selected only by two respondents out of ten.

9. FINAL CONCLUSIONS

Thus, a conclusion that we could draw is that Romanian is pretty close to Hebrew in terms of the linguistic strategies employed. However, the current research also points out to the fact that in Romanian we are more likely to encounter conventional indirect polite strategies compared to Hebrew and English. In this respect, we cannot claim though too much originality of the findings due to the restricted sample of respondents. But if further research will confirm these findings, then this research could be considered a pioneer in the field of applied linguistics and pragmatics. Moreover, we emphasize the idea that only through such research one can actually cover in a scientific manner a part of the challenging field of interculturality, and more specifically of intercultural encounters at the level of linguistic discourse markers.

ENDNOTES

[1] According to Blum Kulka (131), an example of a non-conventional indirect strategy is represented by the category of hints, characterized by lack of pragmatic clarity whereas conventional indirectness is also called "on record" indirectness.

[2] The descriptive categories are similar with those used by Blum Kulka due to the purpose of this paper, i.e. to draw a parallel between three nationalities based on the aforementioned theoretician's findings and this research findings.

[3] Since the respondents were Romanians, and the purpose of the research was to investigate the connection between politeness and indirectness in the Romanian language, the questionnaire was administered in Romanian and the translation tried to be as close as possible to the literal meaning of the English expressions.

REFERENCES

[1] Blum-Kulka, S. (1987) Indirectness and Politeness in request: same or different? in Journal of Pragmatics.

[2] Spencer-Oatey, H. (2005) Politeness, Face and Perceptions of Rapport: Unpakaging their Bases and Interrelationships in Journal of Politeness Research.

[3] Mey,J. (2004) Between culture and pragmatics: Scylla and Charybdis? The precarious conditions of intercultural pragmatics in Intercultural Pragmatics.

[4] Blum-Kulka,S.(1992) The metapragmatics of politeness in Israeli in Trends in linguistics.

APPENDIX

QUESTIONNAIRE

Age:
Education:

Imagine you are in the following situation:

You are asked by your teacher to make some reading notes of the last novel you were supposed to read. You come to school next day and realize that you forgot to do that. You need those reading notes, so you try to get them from your colleagues. What do you say?

Choose from the list below the sentence that seems most appropriate.

1. You'll have to give me your notes. (Va trebui sa-mi dai fisele tale.)

2. Could you give me your notes? (Imi poti da fisele tale?)

3. Give me your lecture notes. (Da-mi fisele tale)

4. I didn't take any notes and I don't want to get a bad mark. (Nu mi-am facut fisele si o sa iau o nota proasta)

5. I would like to ask you to give me your notes.(As vrea sa te rog sa-mi dai fisele tale)

6. I would like you to give me your notes. (As vrea sa-mi dai fisele tale.)

7. How about giving me your notes? (Ce-ar fi sa-mi dai fisele tale?)

8. I'm asking you to give me your notes (Iti cer sa-mi dai fisele tale.)

In the tables below you have the same sentences as above. Number them from 1 to 8.

In Table A, order the sentences on a scale from 1 to 8, where 1 represents the most direct snetence possible and 8 the most indirect one.

In Table B, order the sentences on a scale from 1 to 8, where 1 represents the the most polite sentence and 8 the least polite.

Table A

	Direct
a) You'll have to give me your notes. (Va trebui sa-mi dai fisele tale.)	
b) Could you give me your notes? (Imi poti da fisele tale?)	
c) Give me your lecture notes. (Da-mi fisele tale)	
d) I didn't take any notes and I don't want to get a bad mark. (Nu mi-am facut fisele si o sa iau o nota proasta)	
e) I would like to ask you to give me your notes. (As vrea sa te rog sa-mi dai fisele tale)	
f) I would like you to give me your notes. (As vrea sa-mi dai fisele tale.)	
g) How about giving me your notes? (Ce-ar fi sa-mi dai fisele tale?)	
h) I'm asking you to give me your notes (Iti cer sa-mi dai fisele tale.)	
	Indirect

Table B

	Most polite
a) You'll have to give me your notes. (Va trebui sa-mi dai fisele tale.)	
b) Could you give me your notes? (Imi poti da fisele tale?)	
c) Give me your lecture notes. (Da-mi fisele tale)	
d) I didn't take any notes and I don't want to get a bad mark. (Nu mi-am facut fisele si o sa iau o nota proasta)	
e) I would like to ask you to give me your notes. (As vrea sa te rog sa-mi dai fisele tale)	
f) I would like you to give me your notes. (As vrea sa-mi dai fisele tale.)	
g) How about giving me your notes? (Ce-ar fi sa-mi dai fisele tale?)	
h) I'm asking you to give me your notes (Iti cer sa-mi dai fisele tale.)	
	Least polite

THE RELATIONSHIP BETWEEN PERFORMANCE AND ORGANIZATIONAL CLIMATE

Brînduşa Maria POPA

MSc, Regional Department of Defense Resources Management Studies, Brasov, Romania

The concepts of organizational culture and climate are used to describe the general characteristics of an organization showing the way it behaves in relation to its members. The culture along with the climate influence directly the performance of the organization due to the fact that subjective attitudes and perceceptions of the individuals sometimes clash with the norms established by managers.

Key words: *organizational culture, organizational climate, leadership, performance, change.*

1. ORGANIZATIONAL CULTURE

The analysis of cultural factors (organizational culture and organizational climate) has been frequently used in the last four decades when trying to understand the success or the failure of an organization. Corporates all over the world agree that culture and performance are closely linked and, for this reason, understanding this particular aspect of the organizational life has become a necessity.

The concept of organizational culture was used for the first time by Pettigrew in 1979 in the *"Administrative Science Quarterly"* when he spoke about the economic success of the Japanese firms over the American firms. The success seemed to surge from the motivation of the workers who were committed to a common set of core values, beliefs and assumptions [1]. According to Peters and Waterman [2] successful organizations possess certain cultural traits of excellence thus demonstrating the positive relationship between organizational culture and productivity.

From the analysis of the dynamic relation between the organization and the environment (external or internal) it results that organizational culture is a complex of values, beliefs, ways of thinking and acting which are shared by all the members and which

determine the methods to be used within and outside the organization.

Organizational culture influences directly the performance of an organization and it is the product of the mixture between subjective attitudes and perceceptions of the individuals and norms set out by the management. It is the set of values which determines the behaviour and attitudes that are accepted or not by the members of a group. This set of deep-seated assumptions, values, and beliefs that are enduring, often unconscious, creates the context of activity within organizations and is difficult to change. Maintainig the culture is not as difficult as changing it, this is the reason managers or founders should be careful when they start shaping it. Usually, culture building means attitudes and behavior valued by the founders and later, the things or ways of action encouraged by managers and the conduct which led to successful solutions in the past.

Culture helps people understand the goal alignment and motivates them to higher levels of performance. Having common values, sharing beliefs makes people feel part of the organization and commit their capability and potential totally and willingly for the company. Making the people accept the culture as a result of its understanding will help the organization in challenging or difficult moments. Nevertheless, organizational culture is not the only factor of influence within an organization. There is another aspect which sometimes is included by specialists in the culture: organizational climate. These two concepts are used to describe the general characteristics of an organization showing the way it behaves in relation to its members and explain its success.

2. ORGANIZATIONAL CLIMATE

Organizational climate is the intellectual and moral environment of a group within an organization. Some researchers consider that it should be included in the culture while others see it as being a separate element which needs to be analyzed on its own.

The interest in organizational climate began with the studies made by Lewin in the 50s when he used the concept of social climate. Lewin was interested to see how different styles of leadership affected the attitudes and behaviors of employees and the consequences triggers by this upon the results obtained by the group/ organization. The relation between people and their social environment was expressed as "*behavior is a function between a person and the environment"* [3].

A possible definition of organizational climate could be: an essential element of the social system including all the social characteristics of the interaction between different

workgroups existing within an organization; it is the social and organizational environment in which the groups work and it is determined by the management style.

The difference between organizational climate and organizational culture arises from their degree of stability and persistence. Thus, organizational climate refers to the attitudes and beliefs, the opinions and the sentiments of the employees at a certain moment, while organizational culture rather looks at the values and the elements which are stable and which have a continuity in time (*e.g.* norms, written or not; symbols; values, etc.). Organizational climate is a collective state of the mind which is relatively stable and shared by a group. Organizational culture determines the climate since it is the objective dimension, whereas organizational climate is wreathed in subjectivity. The climate is the key element to be used when trying to understand how the internal environment influences and shapes the opinions, attitudes and behavior of the members. At the same time, through the means of this phenomenon we can decode the dynamics of an organization through the understanding of the subjective perceptions of the employees.

The climate is generally characterised by elements such as: the level of cooperation, of receptivity towards the opinions of the group members, positive atmosphere which could stimulate performance or, on the other hand, tense relations, lack of cooperation, indiference towards performance and other social or professional problems.

Since the effects of organizational climate products can reach an individual or the entire organization, it is vital to be taken into consideration when we aim to attain performance.

Organizational climate depends on several factors that could be generally termed as the characteristics of an organization such as: structure, size, area of activity, age of members and traditions. It also depends on the characteristics of the staff: level of education, age, cultural level and the managerial style.

The culture, seen as a system of interactions through which the subjects coordinate and model each other, has a structure which results from the interdependency of the roles and positions the members have in a group. Taking into consideration the roles and duties each individual has to fulfill we can find several structures which are interrelated and complete each other in accordance with the organizational climate. Groups are made in order to reach some targets or to fulfill some tasks activities which most of the time have a strong motivational load which can influence and even set the way through which an activity is completed.

The group climate will influence and even change the way people behave within a culture and the same

person will have different attitudes dependent on the social environment in which they find themselves at a certain moment. Their reactions change according to the different climates in which they are at that time, or in other words according to the behavior of the other members of the group. Studies have shown that almost all the individuals react similarly to the same group and climate conditions; also, when they change climates the effects are visible even if the organizational culture will remain the same. The differences are visible in the intensity of reactions and in the preference each subject has for a particular climate. So, what could be mistakenly taken as different types of personality or different traits of character is in fact the reaction triggered by the climate and the management method. This is why we should change our perception upon groups as gatherings of individuals and see them as entities which have the capacity to shape the individuals.

The relation between the subjective expectations of the employee and the objective conditions found at the work place, their reaction to the environment is the key to understanding the organizational performance.

When things do not work out, changing culture is much more difficult than changing climate. The premise of the Burke-Litwin model is this: organizational development interventions directed toward structure, management practices, and systems (policies and procedures) result in first-order change; interventions directed toward mission and strategy, leadership, and organization culture result in second-order change [4].

This model differentiates between transactional and transformational leadership styles. In just a few words these two concepts say that some leaders are capable of obtaining extraordinary performance from followers while other leaders are not.

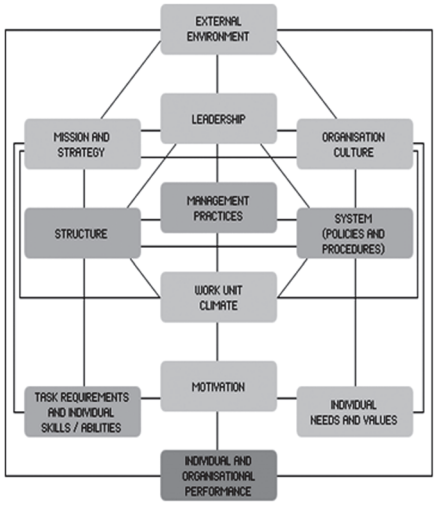

Fig. 1. *Burke-Litwin model of organizational performance and change*

We are talking about transformational leaders, who are leaders who inspire followers surpass their own self-interest for the good of the organization and who are capable of making a strong impression on their followers. Transformational

leadership is about inspiration which helps obtain a higher level of performance, it is about the transformation of the present state into something better.

Transactional leaders are those leaders who guide or motivate their followers in the direction of the goals which were set by clarifying the requirements of the role and task. Transactional leadership requires an exchange of information between leader and follower which will only result in *"normal"* performance. Transactional leadership is sufficient for causing first-order change. Transformational leadership is necessary if we really want to make a difference in the way an organization reaches its objectives.

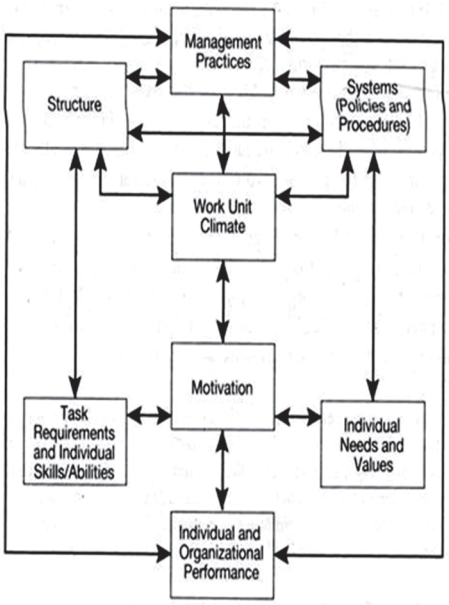

Fig. 2. *The factors involved in first order change*

To conclude, I can say that the employees' attitude towards work is a complex factor. On one hand, it is influenced both by the organizational climate and the organizational culture and, on the other hand, by the style of management. On a general level, the attitude toward work has an impact upon the performance of the organization and on the personal level it influences the employees' individual performance and also their career.

REFERENCES

[1] Denison, D.R. (1990) *Corporate culture and organizational effectiveness*. New York: Wiley.

[2] Peters, T., Waterman, R. (1982) *In Search of Excellence*, New York, London: Harper & Row.

[3] Ostroff, C., Kinicki, A.J., & Tamkins, M.M. (2003) *Organizational culture and climate.* In W.C. Borman, D.R. Ilgen, & R.J. Klimoski (Eds), *Comprehensive Handbook of Psychology*, Volume 12: I/O Psychology, pp. 565-594. New York: John Wiley & Sons.

[4] Burke W., Litwin G. (1992) *A Causal Model of Organizational Performance & Change*, Journal of Management (JofM), 18(3), pp. 523-545.

[5] Vlăsceanu M. (1999) *Organizaţiile şi cultura organizării*, Bucharest: Trei.

[6] Schein E. H. (1992) *Organizational Culture and Leadership*, San Francisco, CA: Jossey-Bass Publishers.

[7] Schein E. H. (2004) *Organizational culture and leadership*, 3rd ed., John Wiley and Sons.

[8] Tomlinson, J. (1999) *Globalization and Culture*, Chicago: University of Chicago Press.

[9] Hall, E.T. (1977/1981) *Beyond Culture*, New York: Doubleday.

[10] Hofstede, G. (2001) *Culture's Consequences: Comparing Values, Behaviors, Institutions And Organisations Across Nations*, Thousand Oaks, CA: Sage, 2001.

[11] Livermore, D., Ang, S., Van Dyne, L. (2009) *Leading with Cultural Intelligence: The New Secret to Success,* Amacom.

[12] Scwartz, S. H. (1999) *A Theory of Cultural values and some Implications for Work,* Applied Psychology: an International Review, Volum 48, Nr. 1, 1999, pp. 23-47.

[13] Foss, N.J., Michailova, S. (2009) *Knowledge Governance: Processes and Perspectives*, Oxford University Press.

[14] Holbeche, L. (2009) *Aligning human resources and business strategy,* 2nd ed., Butterworth- Heinemann.

[15] Marengo, L. (1992) *Coordination and Organizational Learning in the Firm*, Journal of Evolutionary Economics, 1992, Issue 2, pp. 313-26.

[16] Mattson în Drenth, P. J. D., Thierry, H., Wolff, Ch. J. (1998) *Handbook of Work and Organizational Psychology*: Organizational psychology, Psychology Press Ltd.

DEFENSE AND SECURITY EFFECTS OF THE ECONOMIC CRISIS

Maria CONSTANTINESCU

PhD, Regional Department of Defense Resources Management Studies, Brasov, Romania

Following the end of the Cold War and the events at the beginning of the 21st century, the nature of the threats to national security has changed, the single arch-enemy being replaced by a multitude of shifting, sometimes faceless and unpredictable enemies in the form of terrorism, ethnic and religious disputes, trans-national crime etc. Since 2008, a new aspect has been added to the national security and defense, in the form of the negative effects the current economic crisis may have upon these areas.

Key words: *economy, crisis, effects, security, defense*

1. THE ISSUE OF THE ECONOMIC CRISIS

Following the end of the end of the Cold War it appeared that the world was heading towards a brighter future, with the risk of a deadly confrontation between the two rival blocks diminished and the prospect of state cooperation and development. Since then the NATO countries have been faced, individually or as an alliance, with multiple crises and challenges which have transformed the way the areas of security and defense are approached.

The events of 11 September 2001 have outlined the changes in the perceived threats to national and international security, generating the first appeal to the article 5 of the Washington Treaty since NATO's creation, a dramatic shift in the way national defense is perceived and the change in NATO's role and missions. Following these events, the nature of the threats to national security has changed, the single arch-enemy being replaced by a multitude of shifting, sometimes faceless and unpredictable enemies in the form of terrorism, ethnic and religious disputes, trans-national crime, etc.

The traditional view of the defense community regarding the link between economy and defense has sometimes been a rather simplified one, in the sense that the economy was supposed to support the needs of the defense sector through the defense

budget, while some of the activities in the defense area might contribute to the economic development (such as the activities of the national defense industry or potential offset contracts).

This view has been challenged since 2008 as the world and, implicitly, the NATO countries have been faced with the effects of the most serious economic crisis the world has faced since the great depression in the 1930s.

The term economic crisis refers to

"a situation in which the economy of a country experiences a sudden downturn brought on by a financial crisis"...with the most likely effects being "a falling GDP, a drying up of liquidity and rising/falling prices due to inflation/deflation." [1]

Referring to the economic crisis, the economists make a distinction between economic recession and depression. The recession is considered the less serious crisis characterized by a decline in a country's GDP, increase in unemployment and reduced demand, lasting for a relatively short period of time - one year.

On the other hand, the economic depression is an event with more serious effects and lasting for a longer period of time, sometimes several years. The characteristics of an economic depression (as the one triggered by the financial crisis in 2008) include a fall in the GDP lasting for more than 1 year, with negative consequences on the purchasing power of the population generated by reduced wages, followed by a reduced demand and subsequent bankruptcies as the companies see their sales drop. This, in turn, leads to a significant increase in unemployment (generated both through the reduced activity of the business sector but also by the need to cut government expenses). The economic problems are amplified by the contraction of the credit and investment availability, as the general mood of the capital owners is one of caution and aversion to risk and by the decrease in the volume of the international trade and high volatility of the currencies.

2. THE DEFENSE AND SECURITY EFFECTS OF THE ECONOMIC CRISIS

The fall in the GDP, combined with the need to drastically reduce the government expenditures in order to avoid credit defaults has led in many countries to the reduction of defense budgets as the most obvious effect of the economic problems on the security and defense area.

The reduced defense expenditures may have a combined negative effect both at the level of the Alliance and at national level. At NATO level, the member contributions - both direct and indirect - to the NATO common resources may be negatively affected,

as countries may be more reluctant to devote scarce resources to allied missions.

At national level, a short term negative impact of reduced expenditures refers to the national defense capabilities, as the diminished defense budgets determine the military decision makers to take some difficult decisions as to where to allocate the scarce resources. Certain acquisitions of new technologies (especially those of complex or high value weapon systems, such as fighter planes) may have to be postponed or even cancelled due to lack of funds. In certain situations, further measures need to be undertaken, by attempting to prioritize (and reduce) the maintenance and personnel expenses, up to potential downsizing measures of the armed forces.

According to the data published by the European Defense Agency, 16 of the 26 EDA participating Member States have decreased their investment expenses (more exactly equipment procurement and R&D), with an overall decrease from 42 billion EUR in 2008 to 41 million EUR in 2009.[2] In Romania's case, this decrease ha s been even more significant, from 351 million EUR in 2008 to 152 million EUR in 2009, meaning a percentage decrease of 57%, while the biggest reduction in investment expenses has been experienced by Latvia, -75% [3].

Similarly, over the same period, 15 of the 26 EDA participating Member States have decreased their operating and maintenance expenses, with percentages varying from -56% Bulgaria, -41% Romania to -3% Poland.

While some countries, including Romania, chose to decrease the investment, as well the operating and maintenance expenses while maintaining the number of military personnel, other countries responded to the effects of crisis in a different way. Thus, France decreased the military personnel by 30% while increasing the operating and maintenance expenses by 3% and the investment expenses by 11%. Poland decreased the military personnel by 24%, decreased the operating and maintenance expenses by 3% and increased the investment expenses by 22% [4].

Besides the most obvious and direct effects on military budgets, the economic crisis generates other indirect effects, such as a decrease in the demand for the products of the national defense industries, a sharpening of the international competition between armaments manufacturers and a decrease in activity or even bankruptcies for the less competitive. These negative effects would not be confined only to the weapons manufacturers, as other defense contractors, from textiles to electronic components, would see

their business activities slow down due to reduced or cancelled orders from the military.

In this respect, the governments face a difficult choice between protecting strategic national producers and potential negative economic effects of spending even more of the already scarce resources on defense-related areas, in the context of the public debt crisis facing many of the EU countries, amplified by the spectrum of a sovereign debt crisis hanging over some countries such as Greece, Ireland, Spain, Portugal. Both of the circumstances may eventually prove to be a threat to the national security, so the choice is a very difficult one.

Ensuring the necessary level of defense capabilities may be even more difficult as the civil society, faced with increasing economic problems and loss of social safety nets may increasingly question the immediate role and results of defense expenditures when compared to more pressing economic and social problems.

One of the characteristics of an economic depression is unemployment, generated by the decreased economic activity. A high level of unemployment may pose problems in relation to the national security of a country; besides the economic effects of decreased demand for goods and services, lack of revenues for the state from taxes on revenue and the taxes on sales such as VAT, high unemployment has also negative social effects.

Even for the people still employed, the low level of wages (or low level of wage increase), the increased competition on the workforce market, the general decrease in the standard of living, the high level of uncertainty regarding the evolution of the economy, lack of hope for improvement may lead to serious social problems. These are amplified by the government's measures of fiscal consolidation (cut in government expenses, increased taxation etc) in an attempt to counter the public debt crisis, the lack of availability of credit, both to the population and the companies.

The need to control government expenditures is many times reflected in the diminishing of the social expenses, leading to the decrease or even disappearance of social safety nets. Coupled with the obligations to repay the public debt, these measures often lead to discontent from the population which perceives that it has to pay debts which does not concern them, in a general environment of economic and political uncertainty, artificially enhanced sometimes by a media in search of sensational headlines. This discontent, combined with a lack of trust in government and economic authorities may lead to strikes, revolts and other types of sometimes unexpected outburst

of social unrest, such as was the case with the recent revolts in the Middle East (generated partly by economic factors) and even the events in developed countries such as the United Kingdom, with countries with already reduced social spending being at the highest risk.

The high unemployment and reduced social expenditures may be accompanied by a reduction on education expenses. Even if such a measure may seem a good solution to cut costs on short term, on medium and long term it could prove extremely harmful, both to the country's economy and security. An uneducated workforce would be less productive, while at the same time more vulnerable to extremist ideas and actions, leading to additional issues on long term.

Another indirect social effect of the economic crisis with influence on the national security relates to the potential increase in crime, both at national and transnational level, trafficking of goods and persons, accompanied by immigration problems, as many people are determined to leave their home due to economic problems and to seek job opportunities in other countries. Given the fact that the economic crisis effects are not confined to the borders of a single country, the immigrants in search of employment may enter into competition with the local population, leading to an increase in the resentment towards immigrants, followed by social unrests and an increased vulnerability to involvement in terrorist and criminal activities.

3. CONCLUSIONS

Finding the most appropriate ways to deal with the effects of the economic crisis in such a way as to achieve a proper balance between the need to stabilize the economy and the need to maintain the required defense capability and avoid additional national security problems is a challenging issue for any government.

However, despite the difficulty of the task, by careful prioritization of the requirements, an increased emphasis on cost-effectiveness of the government spending and avoidance of *"tunnel vision"* management (focusing just on one area, such as economy, and disregarding the potential implications on other areas such as defense and security) the effects of the economics can be, if not avoided, at least minimized and overcome.

REFERENCES

[1]http://www.businessdictionary.com/definition/economic-crisis.html

[2] http://www.eda.europa.eu/Libraries/Documents/National_Data_Breakdown_Publication_pMS_1.sflb.ashx

[3] idem

[4] idem

[5] http://www.stratfor.com/weekly/20090304_security_implications_global_financial_crisis

[6] Helpdesk Research Report: The Impact of Financial Crises on Conflict and Social Stability, http://www.gsdrc.org/docs/open/HD576.pdf

[7] http://www.nato.int/docu/review/2009/FinancialCrisis/EN/

[8] The Impact of the Financial Crisis on European Defense, http://www.atlantic-community.org/index/view/The_Impact_of_the_Financial_Crisis_on_European_Defense

[9] Biggest Security Threat: Economic Crisis, http://security.nationaljournal.com/2009/03/biggest-security-threat-econom.php

[10] Challenges for European Defense Budgets after the Economic Crisis, http://www.defencetalk.com/challenges-for-european-defense-budgets-after-the-economic-crisis-35589/#ixzz1YOMDX2uI

[11] The Global Financial Crisis: Foreign and Trade Policy Effects, Dick K. Nanto, Coordinator, http://fpc.state.gov/documents/organization/122298.pdf

[12] Security Challenges Arising from the Global Economic Crisis, Dov S. Zakheim, http://www.fpri.org/enotes/200903.zakheim.securityeconomiccrisis.html

[13] The Impact of the Financial and Economic Crisis on European Security and Defence Policy – Challenges and Opportunities, http://www.boell.eu/downloads/Event_Report_Financial_Crisis_ESDP.pdf

[14] The consequences for Europe of the global crisis, http://www.europesworld.org/NewEnglish/Home_old/Article/tabid/191/ArticleType/articleview/ArticleID/21475/Default.aspx

POST-CRISIS PROSPECTS FOR THE MILITARY ORGANIZATION

Codrin HERȚANU

95th Air Flotilla Bacau, Romania

Humankind has constantly evolved for the past two millenia. Even though the term development may suggest a smooth and ascending trajectory, the serious economic problems confronting countries nowadays prove otherwise. Thus, the economic forecasts seem to point out that in the 21st century environmental and resource constraints are to halt the global economic growth. As a result, austerity will reach the military budgets as well, even though the security challenges, both intra and extra-territorial, will remain more or less unchanged, for the next period.

Key words: *strategic concept, global missions, G2, economic crisis, swarming, identification, insurgency.*

1. G2 - THE REAL CRISIS WINNER

The next decade will be a period full of unpredictable events. First of all, Asia will become the leading continent from the economic growing rate perspective, with China and India as main leaders. However, the experts warn us about the instability concerns that usually follow a vast period of steady economic growth. At the same time, the Western countries will go through a period of smooth economic growth. The United States will remain the main world economic and military power, even though the distance between America and its followers, China and India, will lessen.

As the world tends to approach a certain point where the crisis effects will diminish, it seems clearer and clearer that the real winners of the economic crisis are the so-called "G2-group", consisting of United States and China. There are a number of reasons supporting such a statement and some of them are to be presented below.

First of all, China is maintaining its amazing economic rate even though the rest of the world is encountering serious economic troubles.

Second, the other winner, the USA, derives its power mostly form its high posture as an international security defender. Even though the "distance" between United States and its followers will decrease, America will remain the main economic power and the leader of the Western world. The present international security threats request the presence of a leader like the United States, despite the fact that the rest of the world dislikes the United States' involvement in all kind of crises.

Thus, to some extent, one can say that the real crisis' winner is G2. Besides, in the near future, one may witness the establishment of a new strategic partnership including these two states, along with their economic treaties and understandings.

2. LISBON 2010 A NEW BEGINNING

The Lisbon Summit from 2010 might mean a new beginning both for NATO and other relevant defense and security bodies.

First of all, the Alliance tries to develop both a new strategic concept and a new relation with the Russian Federation, as well as new approaches towards Afghanistan stability operations. In this respect, it should be underlined that the Lisbon Summit was a moment when a new strategic consensus emerged that may adjust the structural differences between NATO states members.

Second, new partnerships and global missions were issued. Most importantly, the Lisbon Summit may be the one when the Alliance went back to territorial defense and power balance concept.

Besides all of the above, the NATO-Russia cooperation in Afghanistan gave new dimensions for the Alliance's partnerships. Moreover, the comprehensive approach was the main lesson NATO learnt in Middle East.

All of this tends to emphasize some misunderstandings regarding the complex relationships of the Alliance. Some tendencies were to see NATO as an organisation aiming at Russian Federation and its sphere of influence. In this respect, it should be said the NATO enlargement was a powerful engine of transforming not only the military structures but also the national security cultures. Besides, NATO's role as a strategic balancer, renewed at the Lisbon Summit, will ease the tensions between some Eastern European countries and the Russian Federation.

On the other hand, the solidarity among NATO's member states has always been a issue of huge debates, due to the fact that this kind of solidarity has been seen in different

ways among the respective countries. For instance, for USA and Canada, solidarity means to share costs and operational risks and threats, namely to share money and actions. On the contrary, for some Eastern European countries solidarity is a matter of trust, in other word the answer to the question: "Who may care for my territorial defence and security?" The solution lies in the Article 5 of the Washington Treaty, as well as in trends set forth by the Lisbon Summit to renew the territorial defence main issue.

All in all, it seems that NATO may need a new kind of engagement. The 2010 Summit tried to adjust the solidarity deficiency among NATO states members.

The NATO new Strategic Concept focuses on solidarity, while also establishing a new approach to the Alliance's partnership with the Russian Federation.

3. POST-CRISIS PROSPECTS FOR THE MILITARY ORGANISATION

The present economic crises have shown that to be strong in defense terms does not mean to allocate more resources and to build bigger systems.

However, being cleverer in defense matters might mean to reduce costs. Indeed, there is a need for a better allocation and use of resources. The key is not only the simple change, but the re-design and re-thinking. The Armed Forces of the world need to be re-organized and better equipped with soft power tools in order to counter the emerging threats of today and tomorrow. In the new interconnected war the soft power is better than the hard power and moreover, the military rivalries may be replaced by economic rivalries in the future.

Under the present circumstances, it is most improbable for huge armies of tanks to fight each other in a foreseen conflict since the modern war has become faster and more complex.

The biggest problem at the moment is posed by conventional armies facing the fact that they are organized to fight big wars and, hence, they encounter big difficulties when they are supposed to fight small armies.

The necessities of the big wars made these armies to be based on few big units and not on a lot of small units. For instance, the United States Army has only 10 active divisions and Marines only 3, whereas the Maritime Forces has only 11 groups of carriers. Worth reminding, about 1.5 million people are members of the US Armed Forces.

These underlines the following issue: the US Armed Forces has

a "proper-size" problem, and that makes them unable to follow small targets with small units. The situation in Vietnam was almost the same, when decisional factors forced the Americans to carry on a war with big entities against small insurgents groups. The final outcome is well-known: over 500,000 soldiers deployed in South-East Asia, billions of dollars spent and a lost war.

Nevertheless, some small steps have been already taken to implement the so-called *"more and small ones against the few and big ones' strategy"*. Beginning with 2006 a different operational approach has been in place: 5% of the total 130,000 soldiers in Afghanistan have been disposed in about 100 forward operational posts, consisting of no more than 50 military. That was a spectacular change leading to a decreased level of violence. That was possible due to the fact that the created interconnected network of platoon-level posts was able to interact better with local civilians.

On the other hand, in the second Iraqi War it seemed that the enemy waited for the Coalition forces to arrive and then they ran away, beginning an insurgency based on "hit and run" tactics and attacks with improvised explosive devices.

In current and future conflicts the enemy should be identified first, and then defeated. This was the case in Vietnam and the history has remained more or less the same in Afghanistan and Iraq. In an interconnected war, the massive armies have to adapt themselves from an organization configured to shoot into a more "sensorial" one. This might mean that identification is better than direct attack.

The solution might be the set-up of searchers interconnected groups into the adversary territory, which eventually will co-operate better with the civilian population that hide and protect insurgents.

Terrorists, who know they will never be successful against a regular army, in terms of number, have created a sort of war that allows them to fully benefit from their limited resources. This was called swarming.

Swarming is a tactics of simultaneously attacking from different directions using small units, against one or more targets. After 9/11, Al-Qaeda simultaneously hits targets in Turkey, Tunis and Saudi Arabia, through wave campaign in order to overwhelm the target capacity to react.

Not surprisingly, this kind of tactics, swarming, was used by Russian Federation in Georgia, when federal troops attacked at the same time different targets both on the combat field and in cyber space.

The result was the blocking of Georgian command and control system in several hours. Moreover, the basic services for Georgia's population were blocked within hours using swarming by Russian troops alongside with "friendly" Georgian militia.

Nowadays, the deep implication of swarming could be to adapt the military structure to fight on the combat field with multiple units composed of few trained soldiers. The goal is to trigger rapid attacks, in great number in order to hit enemy in multiple vital points at the same time.

4. CONCLUSIONS

Some contemporary studies underline the similarities between the present world and the one of the year 2025, far beyond the time when the current crisis will lessen its effects. Another relevant aspect emphasised in these forecasts is that the Armed Forces will continue to play a vital role.

New methods of performing asymmetric military actions will be cheaper and affordable. When an unforeseeable conflict cannot be avoided the response will be a key factor in achieving success. Concepts such as: fluid situation, fluid combat actions and fluid battle space will become more common and accessible as part of future military doctrines.

The military structures downsizing will continue in the post-crisis period along with the military cuts in expenditures. However, the efficiency and proficiency of the military structures will increase at the same time. Under the new circumstances, the military combat disposal will be less rigid and will become more asymmetric and fluid.

The new combat space will no longer be uniform and static. On the contrary, this will become more unpredictible and in permanent progress and change.

The military organization will become modular in order to face the combat space digitalization and to be successful in the information and psychological warfare.

As for the military organization as a whole, from the new warfare perspectives to be fluid means to gain mobility, speed and efficiency, to achieve maneuverability and to dominate the adversary battle space. Fluidity also means simultaneous actions in all three batllespace environments: land, maritime and air, performed through joint national/ multinational operations. The means used to accomplish these missions will deliver surgical precision attacks benefiting from high value intelligence provided in real time.

In the near and foreseable future the armies will decrease, some

weapons systems will be forbidden and new arms categories will be implemented. At the same time, both at operational and strategic level, these new systems will be requested to see and strike deep the enemy's decisive points and centers of gravity.

The post-crisis prospects for the military organisation reside in facing the new challenges posed by two future types of confrontation. The first one is that of imposing a new model of world order and globalisation. The other confrontation refers to rejecting the new world order using all available means, from the classical protest to informational warfare and asymmetric retort.

Even though the entire society blames the war and its consequences, the Armed Forces will continue to be prepared for current warfare, but mainly for the future one.

REFERENCES

[1] *** *A National Security Strategy For a New Century*, at the address http:// www.au. af.mil/ au/ awc/awcgate/ nss/nssr-1299.pdf.

[2] *** *Global Trends 2025: A Transformed World,* at the address http://www. ranved. smettef/nat/lad/ poitustajer/greafe/738012.

[3] *** *Foreign Policy,* September/ Octomber 2010, January/February 2011.

[4] Ioan, A. (2009) *Economic Crisis and World Government Reform*, Romanian Military Thinking Review no.1, January-February 2009.

[5] Toffler, Alvin (1996) *War and Anti-War*, Bucharest: ANTET Publishing House.

INSTITUTIONAL COOPERATION BETWEEN ROMANIA AND EUROPEAN UNION IN SOCIAL CRISES PREVENTION

Vasile MESAROŞ

COL. (ret.), Ministry of Administration and Interior, Romania

Romania, as an European Union member, needs to reassess some of its constitutional provisions in order to ensure full alignment of its national institutions to the EU structures. In this respect, some important additions to the Romanian Constitution are mandatory. First, a clear delineation of competences is necessary. Second, the principle of subsidiarity governing the EU exercise of competences should also be part of the Constitution.

Key words: *social crises, prevention, cooperation, European Union, subsidiarity, competences*

Romania, as an European Union member needs to reassess some of its constitutional provisions in order to ensure full alignment of its national institutions to the EU structures. In this respect, some important additions to the Romanian Constitution are mandatory. First, a clear delineation of competences is necessary since, at the level of the EU, there are two types of competences: exclusive and shared. Second, the principle of subsidiarity governing the EU exercise of competences should also be part of the Constitution. Moreover, the same document should set out very clearly the role of the national Parliament in supervising the Romanian Government's application of the European law, as well as in monitoring the correct application of the principle of subsidiarity by the European Union.

The principle of subsidiarity is a feasible and real solution already put into practice in Romania. From this perspective, the subsidiarity should be viewed both as an answer to the growing expectations of citizens to increasingly take part in the making of those decisions that are of direct concern to them, and a necessary debate over the "power" relationships. On the other hand, the subsidiarity is also an organization principle that distributes competences among local, county and national authorities. Moreover, this principle should be viewed as a means to change the manner in which the state acts towards local communities. Thus, besides helping or supporting them, by applying the principle of subsidiarity the state should also encourage their initiatives to find solutions to their own

problems instead of solving these in their place. In other words, the state should "withdraw" itself from the social areas where a community can manage its own current problems. The reasons for such an approach are more than obvious and reside in the fact that a community is more aware of its problems than the central institutions and, therefore, can find better more objective means to solve them.

Obviously, the inclusion in the Romanian Constitution of article 148 in 2003 [1] was necessary and granted Romania's accession to EU. For the time being, the aforementioned article defines the relationship between Romania and the European Union concerning the transfer of some responsibilities to the European Union institutions and the management of the competences listed in the treaties in a shared manner with the other EU member states. Related to these aspects, the Romanian Constitutional Court ruled out that Romania's accession to the EU respects national sovereignty and is a process that allows for a renewed and more complex approach to the latter given the historical circumstances.

However, the collaboration framework among Romanian institutions and between these and their EU counterparts, such as the European Court of Auditors or the European Ombudsman in the field of social crises prevention can be improved.

On the other hand, one must notice that in the EU states community law and national law are interdependent and complementary, and they have some common goals and objectives: the economic development of the member states, as well as ensuring an increasing standard of living for all EU citizens.

Community regulations do not exclude national norms. Every state has the right to develop and implement its own legal framework in order to solve its national issues by observing, at the same time, the general EU requirements. One may rightfully regard this as a correct implementation of the subsidiary principle. The community legal norms and the national norms are thus complementary and address the challenges which Europe faces at the beginning of a new century and millennium.

Our country has made significant efforts to accede the EU, and in doing so it has adopted a new legal framework that is harmonized with the community one, as well as a European-like administrative framework, which address cooperation between Romanian and European institutions in the field of social crises prevention.

After EU accession, the whole national administrative philosophy has to be compatible with the EU's transnational administration. More precisely, an institutional construction must be made to ensure the efficient coordination of the national administrations for the purpose of

preparing Romania to solve the EU-related problems. In order to accomplish this goal, it is necessary to assess the national interests from the community partners' viewpoint: EU Commission, EU Parliament, other member states.

To various extents, the entire national administration is involved in the community's public policies management, whereas the skill transfer at the transnational level makes the line between internal and external policies thinner and thinner in the effort to find common solutions [2]. This process encompasses adapting the Romanian administration to the new realities to achieve performance at the national and community level.

At this moment, Romania has strong democratic institutions engaged in a dynamic process of consolidation and improvement, and are able to sustain the state's normal functioning both inside and within international cooperation activities. The state's institutions must be credible, accountable to the citizens, and endowed with an independent justice system. Also, they must be major landmarks of the state's stability and democracy, in accordance with the values that characterize Romania as a member of international bodies and organizations. From this perspective, any major deviation from providing such a performance in the actions taken by the Romanian institutions can be regarded as a threat to national security. Thus, the risk factors identified in the last years in the proper functioning of democracy and legality, as well as of the strategic components of the state pertain to permanent analysis and action [3].

An efficient and democratic administration implies the radical improvement of the institutional potential at the central and local level, while the sole utilization of the administrative tools, i.e., transparency, correctness and accountability in terms of spending the public money, can effectively contribute to increasing the citizens' standard of living and decreasing the likelihood of social crises. Therefore, public administration bodies must be competent, agile, and adaptable to the new requirements while serving the citizens' interests. On the way to the EU accession, the Romanian institutions had to display the ability to implement the regional development policies and to assure that structural funds should be used totally, efficiently, and legally.

The efficiency of public administration has always been an essential prerequisite of Romanian citizens' security and prosperity. The EU integration process has proved that both the efficiency and the public perception of the administration can be affected by some factors such as corruption, excessive bureaucracy, limited experience in critical fields of activity, unrealistic programs, insufficient authority of justice, public authorities' reduces capacity to manage civil emergencies.

As some of the main pillars of good governance, justice independence and efficiency, as well as the increase

in the people's trust in justice are top priorities meant to guarantee its European quality standards. In the context of this national effort, the state institutions should provide the necessary conditions – legal, organizational, human and material – to support the radical transformation of the state institutions for the purpose of accomplishing Romania's strategic objectives as a EU member state.

Currently, the war on corruption requires that the state institutions should function and be integrated in a system in which vital information circulates in legally and adequately, responsibilities are clear and not redundant, collaboration is tightened among European bodies, and roles are performed timely and legally [4].

For a better understanding of the state's current situation in the new international context and its interdependencies with the transnational organizations, one should comprehend the three-stage process of the state transformation and adaptation: at the political level, from a subjects' state to a citizens' state; at the economic level, from an autarchic state to an interdependent state; at the symbolic level, from a state in charge with providing physical security to a state in charge with providing its citizens' economic and social security.

As far as the EU is concerned and according to the principle of subsidiary, the member states commonly decide upon the problems that are better solved at that level than the national level. If decisions prove to be more efficient at the state or regional level, that is, more closely to the citizens, than they must be taken without the EU interference [5]. Consequently, the EU states have delegated part of their power to the EU, and decisions of common interest are made at the community level.

The three main decision-making institutions are: the European Parliament, which represents the EU citizens and is elected by them, the EU Council, which represents the member states, and the European Commission, which pursues the EU interests. This institutional triangle develops policies and adopts documents (regulations, directives, decisions, etc.) applied in the entire EU. The EU norm application is supervised by the Court of Justice, whereas the financial part is verified by the European Court of Audit.

The relationships between the EU and Romanian institutions are based on partnership, cooperation and mutual advantages. Their objective is to increase the citizens' social, economic and cultural wellbeing, to promote peace and social-economic development all over Europe and worldwide. Ever since it was set up in 1957, the European Parliament fully participates in developing community legislation and in managing the EU. The European Parliament exerts three fundamental powers: legislative, budgetary and control over the executive.

The goals of the European politics are to go beyond the boundaries of

the social and economic framework established by the community treaties and to achieve a common strategy in preventing the social crises, as well as many other fields of activity such as war on drugs, fraud and international crime.

In addition to the aforementioned aspects, the EU Parliament pays special attention to human rights in Europe and all over the world, with an emphasis on social, economic, political aspects which are referred to in six main chapters: dignity, freedom, equality, solidarity, citizenship and justice.

As far as the strategic goal of solidarity and prevention of social crises is concerned, the most important topics approached by the Parliament included: demographic challenges and solidarity between generations, sustainable economic growth and the use of labor force, social and economic impact of enterprise restructuring in Europe (particularly in the car industry), social protection and integration, effects of globalization on the internal market [6].

The EU Council, also known as the Council of Ministers, has no equivalent. The EU member states issue laws, establish policy objectives, coordinate national policies and solve disagreements between them and other institutions. One may state that the EU Council sometimes displays the characteristics of a transnational organization, and some other times it displays the characteristics of an intergovernmental organization. Besides, it comprises the representatives of every member state at the ministry level.

On the grounds of the European Community establishment treaty, the Council has the following responsibilities: it is the European Community's legislative body with regard to a wide range of aspects; it coordinates the member states' general economic policy; it secures international agreements on behalf of the community; together with the European Parliament it is the community's budgetary authority [7].

The EU Council adopts the following documents, which become mandatory for all the members: regulations, which are applicable everywhere and in the most comprehensive way; directives, which harmonize the members' goals and objectives, but allow them, at the same time, to choose the methods to achieve these goals and objectives. This means that the national governments need to take measures to put in practice these documents.

The European Council comprises the chiefs of the 27 EU states and/or governments and the president of the European Commission. It is not the same as the Council of Europe, which is an international body; nor is it the same as the Council of United Europe, which consists of ministers. From a legal point of view, the European Council is not an institution of the European Communities, but it plays an important role in all the EU's fields of activity by defining the general political trends [8]

or by providing solutions to difficult problems such as social crises.

The European Commission represents the common interest and personality of the union, with an emphasis on protecting its citizens' interests. Its role is to ensure the free circulation of goods, services, capitals and people across the EU territory. The commission is the EU engine: it elaborates legislative proposals and supervises their practical application. Also, it acts as an executive body meant to manage and implement the EU budgetary policies.

Apart from the institutions previously presented, there are other bodies, offices, and agencies at the EU level that represent the members' social, economic and regional interests: consultative bodies (Economic and Social Committee, Regions Committee), financial bodies (European Banks of Investments, Central European Bank), control bodies (European Ombudsman, European Control for Data Protection), subsidiary offices and agencies, inter-institutional offices and agencies, decentralized offices and agencies, personnel selection offices, administration schools, foundations, authorities, etc.

REFERENCES

[1] *** (2003) The Constitution of Romania, Bucharest, p. 62.

[2] Nastase, Adrian (2007) European Romania, Bucharest: MondoMedia Publishing House, p. 165.

[3] *** Romania's Government, Governing program 2009-2012, pp. 45-46.

[4] Voicu, Costica et al. (2006) *Organized business crime*, Plindner & Plindner Publishing House, p. 293.

[5] Gabriela Gabor (coord.) (2003) *Romanian identity and European integration*, Bucharest: Ars Docenti Publishing House, pp. 34-35.

[6] *** http:/europa.eu, General report on the EU activity, 16.04.2011.

[7] Profiroiu, Marius (coord.) (2008) *European institutions and policies,* Bucharest: Economica Publishing House, p. 59.

[8] *** http://search.incredimail.com, EU Charter,Article 4 of the EU Treaty.