Information & Security Volume 5, 2000

C4 in Defense Reengineering

Edited by Velizar Shalamanov

I&S Monitor

I&S Library Update

I&S News

Author: **Editorial**
Title: **Reengineering Defense: The Role of C4**
Year of issuance: **2000**
Issue: **Information & Security. Volume 5, 2000**
Hard copy: **ISSN 1311-1493**

REENGINEERING DEFENSE:

THE ROLE OF C4

Significant changes occur in post-communist societies. Most notably, the changes are characterized by remarkable scale, depth, and speed. This is especially true for the change in the area of defense and security. Roles and missions, force structure, equipment, doctrine and training are all being redefined. The current situation is typical of the process of reengineering. According to the definition by Dr. Hammer, reengineering is "… the fundamental rethinking and radical redesign of business processes to achieve dramatic improvements in critical, contemporary measures of performance, such as cost, quality, service, and speed." Almost three years ago, Bulgaria launched the reform in defense and security adhering to the formula "success = leadership + reengineering + IT." Now, accounting to the experience gained in defense reform, the formula for this area is a little different: "success = democratic control of armed forces (top-down) + Command, Control, Communications, Computers (bottom-up) + education and training, research and development aimed at manning the system with quality people, equipment and procedures."

The purpose of the articles in this issue of *Information & Security* is to present our Vision, Will, Confidence and Capability to implement the above formulas in the area of C4. The goal will be achieved with a set of papers on different issues and focused on different aspects of the C4 life cycle and C4 dimensions prepared by people who were directly involved in the process during recent years as members of distributed and integrated teams.

The first article in this volume provides a comprehensive, if no detailed, account of the changes in the area of defense and security in Bulgaria, with emphasis on the particular role information technologies played—and continue to play—in this endeavor. The account is provided by Dr. Velizar Shalamanov – Deputy Minister of Defense, Plans, and Policy, and one of the leaders and visionaries for the future of Bulgarian defense.

A group of articles presents the policy for developing and implementing Command, Control, Communications, Computers and Intelligence (C4I) systems under strict resource constraints. Mr. Loren Diedrichsen presents the fundamentals of using C4 in the defense reform process. His article covers issues in three areas of decision-making as formulated during his lecture in Defense College in Sofia:

- Studies to provide basis for fundamental rethinking (informational decisions);
- Documents and organizational structures to support the process (organizational

decisions);

- Action plan for the process (operational decisions).

There are different aspects of the role of C4 in defense reform. Broadly, C4 includes not only communications and information systems (CIS) but also the set of decision-making and information management processes that are known as Command and Control (C2). Therefore, C4 covers even the knowledge base of defense reengineering, and in many publications the Chief Information Officer (CIO) is referred to as "Chief Knowledge Officer (CKO)." In this case C4 can be considered as process with many steps and elements:

- Definition of goals and vision;
- Studies conducted by integrated joint teams to define variants for defense reform, including all types of R&D required;
- Selection of optimal variant and development of plans;
- Programming – linking goals, results, resources in a time frame;
- Program management;
- Education and training;
- Development of C4 for defense system;
- CIS support of the above processes.

Therefore, C4 is essential for the reengineering of all aspects of the defense process: fundamental rethinking, radical redesign of business processes, implementation to achieve dramatic improvements in critical measures of performance such as cost, quality, service, speed, progress measurement and assessment of success.

Reengineering of the C4 area itself is "recursive" in relation to what we discussed above. It means that we can test the approach in the C4 area and, when success is achieved there, to accelerate processes in other areas supported by C4 through application of lessons learned from C4 experience. C4 is critical to the two other elements of the "success formula" - democratic control (transparency) and E&T/R&D. Having "strong" C4, it is possible to support and track effective decision making and effective education and research. Because it is of such importance, the issue of security (information assurance) becomes crucial - "small mistakes" can influence too many important decisions and to become a "real and present" threat to the overall process of defense reengineering.

These are preliminary thoughts about the role of C4 in defense reengineering. It will be interesting to develop a more comprehensive theory of this phenomenon, but currently our goal is to start the presentation of empirical experience of the Bulgarian MoD during the last three years based on the following steps:

- Study of the defense reform;

- Study of the organizational structures and their performance;
- Study of C4 systems;
- Study of the Air Defense System;
- Introduction of the PPBS system for resource management;
- Introduction of the C4 systems life cycle support model, CIO institution and integrated management structures;
- Introduction of an integration "roadmap" based on joint technical architecture and common operating environment;
- Introduction of the integrated E&T / R&D model based on "massive use" of CIS for modeling and simulation, distance learning, Computer Aided Exercises, Computer Aided Engineering, testbed / evolutionary development facilities, Internet/Intranet, etc.;
- Introduction of a common strategy for information assurance.

It is important to stress that although the above steps, successfully implemented in the MoD of Bulgaria, were entirely a national responsibility, they were effectively supported by close cooperation through foreign consultancy and assistance programs. The next step, already underway, is to implement this experience in other government agencies, that is, to support national reengineering efforts and the building of the Information Society in Bulgaria.

Papers included in this issue of the journal will highlight some aspects connected with the development of the roadmap for reforming C4, operational requirements and system implementation of advanced command and control, C4 architectural frameworks in coalition environments, practical dimensions of information support for decision-making during the Kosovo crisis, the application of advanced IT in the context of participation in the Consortium of Defense Academies and Security Studies Institutes, and the engagement of MoD in the building of the Information Society. The next volume of the journal will provide details on the implementation of the C4 policy in particular projects.

We believe that these initiatives that became possible during last three years will facilitate the implementation and integration of defense reform plans and will be of interest to other countries undergoing similar transition. The discussion started with this volume can be reinforced by a conference on the two aspects of the task: the purely technical aspects of C4 life cycle support and, more broadly, the C4 implications of democratic control of the security sector, education and training, research and development. Any feedback on the above spectrum of problems will be greatly appreciated.

BACK TO TOP

Information & Security. An International Journal
e-mail: infosec@mbox.digsys.bg

Author:**Velizar Shalamanov**
Title: **Lessons of Transition in Bulgarian Security and Defense**
Year of issuance: **2000**
Issue: **Information & Security. Volume 5, 2000**
Hard copy: **ISSN 1311-1493**

LESSONS OF TRANSITION IN BULGARIAN SECURITY AND DEFENSE

Velizar SHALAMANOV

Table Of Contents:

Introduction

A little over two years ago this journal published a translation of the famous article by Prof. Jeffrey Simon "Bulgaria and NATO: 7 lost years." [1] Now, it can be stated that for less than three years the better part of the needed steps for the last ten years in the "information domain" were taken. The "magic formula" of democratic control of armed forces that provides transparency, cooperation and public support, as well as modern study methods, IT, new type of education, training and research is to prove that this transition is highly information intensive process. Any serious change simply needs preparation and a plan. Although changes are on different levels, in different areas, information and knowledge integrate all of them and management of change is again primarily seen as information/knowledge management.

The transition from armed forces, that used to be part of the Warsaw Pact military machine, designed and controlled by Moscow, to a new type of armed forces capable of responding adequately to the new reality, is a serious challenge to the post-communist militaries. This new type of armed forces has to be governed by the principles of democratic civilian control and be part of a larger international security system. In addition to national defense, they have to perform a number of new tasks related to

early warning, crisis prevention and management through military operations other than war (MOOTW) performed by combined joint task forces (CJTF).

There are different sets of criteria to highlight the transition of post-communists militaries developed in OSCE, NATO/PfP, based on the experience of NATO accession process and from the experience of different democratic countries that started some kind of defense diplomacy programs to support this transition period.

The OSCE criteria for effective civilian control of the armed forces were presented in 1995: clear, constitutionally defined distribution of responsibilities; parliamentarian oversight, approval of the budget and control of its implementation; civilian control of the military through a civilian minister and civilian staff capable of analyzing the budget, defense plans and programs, force structure and intelligence activity; armed forces that are an effective institution serving the society under the control of elected civilians and tasked with the protection of national security and participation in MOOTW.

The Partnership for Peace Program, launched in 1994, is instrumental in achieving desired status. The recently published transatlantic strategy of the United States [2] provides a very simple definition of the PfP core objectives:

- Facilitate transparency in national defense planning and budgeting processes;
- Ensure democratic control of defense forces;
- Maintain capability and readiness to contribute to crisis response operations under the appropriate international mandate;
- Develop forces that are better able to operate with those of NATO members.

Similar to these are Secretary Perry's NATO accession criteria: democracy, market economy, good relations with neighbors, reform to build military capabilities, and democratic control of the armed forces. They are further developed in the Membership Action Plan (MAP) process on the basis of the accession experience of the first three former Warsaw Pact countries – the Czech Republic, Hungary and Poland – that joined NATO.

The transition of post-communists armed forces is a process, running parallel to the transition to democracy, market economy, and the rule of law in the respective countries.

In some aspects, the military transition is better to be considered in the larger context of the reform of the security sector, including reform of secret services, internal security and civil protection. On the one hand, this area is considered as a sector that is well organized and easy to control, but on the other hand, the establishment of democratic control is difficult for a number of reasons. Practically speaking, key elements of the process include political guidance and civilian control, introduction of modern management and information technologies (including PPBS-type of planning) and intensive education and training combined with a smart personnel policy. The attempts to assign the responsibility of transition to purely military organizations (for example the General Staff of the respective military force) were mostly unsuccessful.

There are many lessons learned, that can be arranged in three levels:

- Redefinition of security and defense: from block confrontation to security and defense through cooperation and integration;
- Redefinition of the role of the military in the state – to provide security and defense and to support development of the country and its cooperation, the integration in the democratic, market oriented community of prosperous states;
- And on the basis of the previous two - to define the scope and depth of defense reform to support the national objectives.

Following are some thoughts in these three areas based mostly on the Bulgarian experience. We believe they reflect relatively common lessons and can be used as a basis for discussion. It is convenient, that this experience is well documented in a series of official security and defense related documents and, more importantly, in accounts of many studies performed by international teams, in itself a dimension of transparency. The study teams used modern information technologies, thus indicating the importance of IT for management of change. Study results and methodologies were often directly included in the education and training processes, which also proves how crucial all this is.

And yet, this process is a "two-way street" issue. There are some initiatives from Western countries, started as common to all militaries in transition, but later adjusted to each country on the basis of its particular experience, the latter being the most important factor for success. Therefore, my intention is to analyze not the Western, but our part of the transition efforts and stress on the fact that they are a national responsibility, based on national resources, including the human ones. Having this in mind, I would like to emphasize that without a great initial support it was impossible to get where we are now. Future progress will inevitably involve IT, education and training (E&T), research and development (R&D), improved planning, intensive cooperation and integration processes.

The role of security and defense in South East Europe (SEE) and the countries in transition

During the period of block confrontation, Bulgarian security and defense were guaranteed by the Warsaw Pact. After its dissolution several different options were explored by Bulgarian society: from neutrality, through regional alliances and bilateral agreements, to NATO accession. Now it is clear that the ambiguity of that situation was contemptible for the military, but at the same time they were not prepared to offer professional military assessment of the different options (including resources and other external implications) in order to support the decision-making process. There was no proactive approach of the military that had been indoctrinated in the Soviet-style command and control system. At the same time, there was no civilian expertise and commitment to formulate a totally new concept and doctrine for the security and defense of the country.

Parallel to this, there was a process of transition to a system of civilian control. However, due to the lack of expertise in the civilian bodies, the lack of will in the political bodies and a certain level of encapsulation of militaries determined to keep the system as it was, the process was mutually blocked on a very high level. Lower levels were suppressed not to put at stake the imaginary stability.

Having no National Security Concept (National Security Strategy) and Military Doctrine (National Military Strategy) all reform attempts, covered by the Law on Defense and Armed Forces and the Manual for Career Development of Cadre Military, aimed at adapting to current situation. They rarely had any positive effect and caused a serious damage to the potential for change and development.

The first positive step was taken with the decision of the Government, dated 17 February 1997, to apply for NATO membership, followed by the first National Program for NATO Accession, adopted on March 17, 1997. It was further built on by the National Security Concept of the Republic of Bulgaria, approved by the Parliament in 1998 and estimated as real national achievement.

The lessons on this level include:

- Security and defense issues cannot be decided in secrecy by military professionals. These are "too serious problems to be addressed by generals alone";
- Security and defense are closely related to the vision on the overall development of the country. They are an issue of civilization choice, an issue of values;
- Security and defense are essential for the country, because they are a prerequisite for development (they are an investment in security and guarantee security of investments), but at the same time security and defense compete for the same limited resources with other state priorities. Balance, mutual support and synergy are crucial;
- Critical mass of experts – in society (NGOs, media, universities), in the ministries of defense, foreign affairs, and finance, in other government agencies and in Parliament, as well as the ones involved in close international cooperation – is needed to start the reform process;
- E&T programs of Western countries and organizations were an important investment, but internal motivation and commitment of more and more Bulgarians was the decisive factor to overcome the inertia and the lasting sabotage of the former secret services.

All these lessons can be used to further outreach programs of introducing in more states national security concepts harmonized with those of the democratic community. This process is connected with deep and informative debate. Media, Internet, E&T, R&D programs, joint studies are very important, and the supporting role of IT is indispensable.

The role of the military in the democratic states

The role of the military in a democratic society is extremely important and prestigious, but it is rather different from the one that existed during the totalitarian period. Having redefined security and defense on the political level, we found ourselves in a situation where there was a gap between new political framework and the existing military establishment. The role required by the state was

difficult to be played by unreformed military, and the role that the unreformed military wanted to play was unacceptable for the state and society.

Within the framework of the above mentioned features of the transformation of post-communist militaries, hard work was needed to define this new role, and to persuade the society and the military that this is of mutual interest. To persuade them that changes are difficult but need to be done for the sake of the country.

A lot of time was lost and, as a result, when realities started to require real military capabilities (not on paper), it became clear that there was no package of military capabilities, adequate to the resources and public support. Practically all plans were driven by the idea to keep large armed forces, even at the cost of no modernization, poor training levels and very limited crisis management capabilities. At the same time, the security environment was changing and the requirements to force structure, equipment, training, doctrines and, most of all, early warning and rapid reaction in unpredictable situations, became critical.

It was impossible to accomplish real reengineering of defense and armed forces with the armed forces' own resources. All proposals presented variations of the same structure, equipment, training and doctrines with unrealistic financial implications. There was resistance to initiate an in-depth strategic defense review with the assumption that there was no alternative to the General Staff in doing this; and if they were not the ones doing the review, the framework would be kept unchanged.

However, things started to change with the adoption of the National Security Concept, the direct involvement of the Prime Minister and the series of joint studies within the strategic defense review framework. The new security and defense structure was built on three pillars – cooperation, integration and optimal military capabilities, the first two actually being a catalyst to the strengthening of the third one.

The irreversibility of the change was also reinforced by the Military Doctrine of the Republic of Bulgaria. It was approved by Parliament in 1999 and proved adequate by the Kosovo crisis and the Washington Summit outcomes. The Military Doctrine and the Crisis Management Concept were the documents that framed the mature behavior of Bulgaria during the Kosovo crisis.

The main lessons on this level include:

- It is the responsibility of the civilians and society to define the role of the military in the national security system;
- Any kind of defense reform without political guidance and civilian control is simply a waste of time, resources and confidence in the transition efforts;
- Civilian authorities cannot fulfill their responsibilities without a strong analytical support, control of the military education and personnel policy, as well as without a system for strengthening the public support;
- Two-level integration (between civilians and military, and between national and

foreign experts) is possible only after developing a certain capacity in the differentiation phase (a separate capacity for civilian and military, for national and foreign experts). Only after that, and on the basis of a clear statement of work (SOW), high level approval and under tight political control joint teams can start working effectively;

- A clear system of measuring the military activity and real use of military capabilities – exercises, crisis management, MOOTW, etc., is essential to define and prove the new role of the military;
- Cooperation and integration processes, force structure, equipment, doctrines, training, education and personnel policy embedded within the PPBS are powerful tools to redefine the role of the military;
- Policy guidance and control is a responsibility of the civilians, the implementation - of the military, and the kernel – planning and programming – is a joint activity.

All these lessons need IT for effective implementation. At the same time, successful accomplishment of the above changes provides environment for effective implementation of modern IT.

Milestones of the transition process

This is the third level – the level of practical implementation of the above mentioned principles and documents which proves how crucial the democratic control of armed forces is.

Following is only a short description of the transition phases of the Bulgarian experience:

1990-1996:

Waiting for political guidance, full dominance of the General Staff, preservation of old structures, erroneous procurement policy, exhausting of reserves, sporadic bilateral cooperation, formal participation in international organizations:

- New Law on Defense and Armed Forces, 1995; Amended in 1996.

1997-1998:

Clear political will, shaping the political framework, lack of competence of the civilian administration of the MoD, more open bilateral and regional cooperation, vitalization in the area of integration on political level:

- Declaration of Determination to join NATO, February 1997;
- Creation of Inter-ministerial Committee for NATO integration, February 1997;
- First National NATO Accession Program, March 1997;

- "Reform Plan 2010," 1998;
- First National Security Concept, April 1998;
- Amendments to the Law on Defense and Armed Forces, 1997, 1998.

1999-current:

Direct involvement in the defense reform of the Government and the Prime Minister through the Security Council; building internal capacity for strategic defense review and defense planning, increased integration of the Ministry of Defense and the General Staff, development of realistic reform and integration plans, proactive regional and integration policy:

- Joint US-Bulgarian Defense Reform Study, 1999;
- Crisis Management Concept, March 1999;
- First Military Doctrine of the Republic of Bulgaria, April 1999;
- Defense Reform "Plan 2004," October 1999;
- Bulgarian Membership Action Plan, October 1999;
- C4, Air Defense, Civil-Military Relations /Integrated MoD/ studies, 1999-2000;
- "Organic Law" of the MoD, defining organizational structure and functions of the administration, 1999;
- New Manual on Career Development of Cadre Military;
- Amendments to the Law on Defense and Armed Forces, 2000;
- Mid-term departmental plan organized in 21 comprehensive programs, 1999, 2000;
- First annual reports on National Security and on Status of Defense and Armed Forces, 2000;
- Full harmonization of the national and NATO defense planning, 2001;
- First draft version of White Paper on Defense and Armed Forces, January 2001.

A short analysis of the bullets (even only of their number, not content) can give a clear idea for the importance of democratic control of armed forces and mature civil-military relations. An in-depth content analysis is a serious task that can lead us to extremely important lessons about the national defense policy and defense diplomacy, but this is a topic for another study.

Following one full year of implementation of the above documents, plans and programs, there are many lessons learned, but it is important to stress that they are just to prove the importance of the principles listed in the introduction.

These lessons include:

- Crucial role of political guidance, will and control;
- Requirement to delegate decision making authority and control;
- Key role of programming in linking results to resources within an adequate time frame;
- Essential role of the new information technologies – communications, computers and decision support tools, as well as R&D in all defense reform related areas;
- Critical role of education, training and personnel policy – to select and motivate the right people;
- The importance of the ownership of the processes by right level people;
- The decisive role of progress reports to control the process and gain support and motivation.

To a great extent these lessons were taken into account and incorporated in the Reform Plan 2004 and the Membership Action Plan of the Republic of Bulgaria approved by the Government in 1999; the Bulgarian system for planning, programming and budgeting; the reform initiated in the field of E&T and R&D; the establishment of "Chief Information Officer" and the elaboration of the respective manual for life cycle support of C4 systems in the MoD. [3]

This is a "live" process and the permanent improvement and management of the change is something that needs continuity and commitment. Many processes underway are result of compromises that only people deeply involved are aware of. Therefore, it is extremely important to keep teams together. The old thinking that everything can be put on paper and after that implemented by other people without permanent improvement of the "fathers" is dangerous for the fragile transition. As the military say, "Plans are nothing, planning is everything", so keep planning and implementing – management of change by a strong team, supported by effective information systems and solid political and public support.

Conclusion

The main lesson is that transition will never come to an end but there will always be a constant development and progress. The implementation of Plan 2004 and the MAP, the accession to NATO and the EU are only milestones of a long journey to better security through cooperation and integration that will provide opportunities for prosperity of more people as well. In order to support this process we give priority to the improvement of the system for democratic control of armed forces and the security sector as a whole. This will introduce transparency, accountability, effectiveness and efficiency through our PPBS, strengthening the implementation of modern management and information technologies and excellence in our E&T / R&D system.

Gaining political and public support for the transition is crucial. After four years of serious efforts we are really close to understanding our own lessons. Together with our people, this is the most valuable

asset for the most serious part of the Bulgarian transition – receiving an invitation to join NATO and finalizing the process of building the first military blocks to contribute within the Alliance New Strategic Concept.

The success story of Bulgaria has proved that military reform efforts have a great potential when they are proactive and linked to the overall integration processes throughout Europe.

It is important to stress that reform is like love - it's a journey, not a destination…

To achieve your destination, though, you need appropriate speed, determination and clear perspective as to where your heart and mind drive you. And if you need a formula for military reform, go back to Benjamin Disraelie's definition: "The secret of success is constancy of purpose."

In the past it was stated that the direction was important, not the speed. Now, in the information age, in the age of change, it is not only the direction and the speed that are the most important; it is the acceleration. And, of course, the purpose has to be the same – more security and prosperity for more people. This purpose is essential for the transition of post-communist militaries and it is the responsibility of elected civilians (consulted by military and civilian professionals) to guide the execution by military professionals and to provide public support for the process.

Transition is impossible in isolation. Success in security and defense reform requires synergy of effort in international cooperation and integration endeavors, transparency through systemic democratic control of armed forces, effective implementation of new IT, developing the foundation for the future through education and training, R&D, and, finally, constantly measuring progress both in formal and informal ways, as well as through participation in real-world crisis management operations.

Acknowledgment. The most intensive period of the changes started at the end of 1998. Genuine defense reform was possible because of the commitment, intellectual effort, and hard work of many young, motivated and well-educated people, who became part of the defense policy and planning sector of the Ministry of Defense. But it is not possible to name everyone who spent long work hours and many weekends away from their families. Invaluable was the assistance of experienced specialists of the Ministry of Defense and the General Staff, who decided to open a new page in their endeavors. Many people from outside the Ministry of Defense contributed and, of course, the support of Government, Parliament and society was crucial. This is probably the first time when Bulgarian society was so actively involved in planning and implementing security and defense reform. The role of the joint studies and foreign consultants is difficult to measure, but their significance is beyond doubt.

References:

1. Jeffrey Simon "Bulgaria and NATO: 7 lost years," *Strategic Forum*, No. 142. Published in Bulgarian in *Information & Security. An International Journal* 1, 2 (Fall, Winter 1998), 93-104.

2. *Strengthening Transatlantic Security: A U.S. Strategy for the 21st Century* (Washington, DC: Department of Defense, December 2000).

3. Described in detail in articles in this volume.

Dr. VELIZAR SHALAMANOV is Deputy Minister of Defense for Defense Policy and Planning since November 1998. He holds the title of Associate Professor on automated information processing systems (Computer Science and Operations Research) and has with more than 120 publications in areas of CIS architecture and development, IW, decision support, national and regional security policy, military art, defense reengineering, defense planning, democratic control of armed forces and security sector, defense R&D, education and training. Dr. Shalamanov is member and co-founder of AFCEA-Sofia Chapter, member of Council of Geneva Center for Democratic Control of Armed Forces, member of Bulgarian Coordinating Council on the Problems of Information Society and Bulgarian Interagency Committee for NATO Integration, as well as of other national and international institutions. E-mail: shalamav@md.government.bg; shalamav@bg.pims.org.

BACK TO TOP

Lessons of Transition in Bulgarian Security and Defense

Velizar Shalamanov

Keywords: Civil-military relations, security sector reform, strategic defense review

Abstract: Advancement of information technologies, and in particular TV networks and Internet, contributed to the fall of communism in Central and Eastern Europe. But the transition to democracy, market economy and civil society is a complex process with specific ups and downs in each country. One of its components is the transition in the area of security and defense - highly information intensive process. This article describes lessons learned form the transition of the security and defense sector in Bulgaria and outlines major requirements for further evolution towards full integration in European and Euroatlantic security and defense.

Author: **Loren Diedrichsen**
Title: **Command & Control: Operational Requirements and System Implementation**
Year of issuance: **2000**
Issue: **Information & Security. Volume 5, 2000**
Hard copy: **ISSN 1311-1493**

COMMAND & CONTROL

OPERATIONAL REQUIREMENTS AND SYSTEM IMPLEMENTATION

Loren D. DIEDRICHSEN

Table Of Contents:

Introduction

The objective of this paper is to examine the accepted definition of "Command and Control" (C2), and from that examination to derive the fundamental operational requirements for a Command and Control Information System, to outline the operational, system, and technical architectures for such a System, and to put forward a basis for the evolutionary implementation of an effective Command and Control capability that extends over all levels of national command.

Acknowledgements

My formulation of the fundamental requirements for a military Command and Control System is based to a large degree on the theoretical foundation for Command and Control presented in the excellent practical textbook entitled: "Command and Control, The Literature and Commentaries" authored by Mr. Frank Snyder,[1] of the USA National Defense University and the Director of its Command and Control Research Program. I have also taken into account the views and experiences contained in an AFCEA International Press book, entitled: "Principles of Command and Control."[2]

US DoD Definition

The US Department of Defense defines "Command and Control" as follows:

> "Command and Control is the exercise of authority and direction by a properly designated Commander over assigned forces in the accomplishment of the mission. Command and Control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures which are employed by a Commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission."

"Command and Control" is the critical process employed by military commanders when exercising military power to achieve national objectives.

Command Structure

A Commander's authority is derived from a hierarchical command structure, which links the National Command Authority (for example, the head of government), through a formal military structure comprising the operational commanders having the ability to apply military power. This hierarchical command structure provides a top-down allocation of authority and responsibility to subordinate military forces, which maximizes the probability of success in mission accomplishment, while minimizing operational risk. The command structure must create and establish workable command relationships throughout the chain of command, and provide a clear definition of the functions to be performed at each echelon within that chain of command. This national Command and Control structure can be considered as having four command levels; namely National, Strategic, Operational, and Tactical.

Military Situations

Command and Control is a continuous process exercised over the complete range of situations under which a nation may decide to apply military power to achieve its national objectives. This range of situations includes: Peacetime; Military Support for Humanitarian Relief or National Civil Crises; Peace Support including peacekeeping, peace enforcement, and peacemaking; Limited War; and General War.

Military authority and direction, associated with the application of military power for each of these situations, flows from the National Command Authority through the hierarchical Command and Control structure. In each of these military situations, the appropriate command relationships must be established through the chain of command, and the functions that are to be accomplished by each command element must be clearly defined.

Command Control Process

Much has been written of the need to carry out extensive studies to define the "information exchange requirements" for a Command and Control System. I believe that there is a fundamental flaw in this type of thinking. Decision-making, not information flow, is at the heart of the command and control process. The decision-making process of command and control is very much an iterative process, strongly supported by inputs from specialist staff that address a range of "what if" questions posed by either the commander or his senior advisors. From historical studies of past military operations, we know that decision-making for command and control also involves an aspect of chess playing as commanders plot their moves and make their decisions in the context of at least a two party conflict situation, wherein each opponent is doing the same. Any attempt to define precisely the information exchange requirements for a command and control system is limited by the inability to formulate the broad range of potential questions or issues that would be addressed during the C2 decision-making processes, associated with the entire range of military situations.

A Command and Control Information System must be designed first and foremost to provide effective and responsive decision support. To achieve that goal, the system must include support for the staff whose mission it is to provide the various inputs needed for command and control decision-making, some driven by the functional responsibilities of the staff and others driven by specific queries posed by the Commander. The system must enable the staff to access any relevant information, no matter where that information might reside in the network. This is the fundamental basis for the concept of "network-centric".

Although the focus of decision-making in Command and Control differs at the National, Strategic, Operational, and Tactical levels of command, certain of the data and information products, although used differently, are associated with decision-making at more than one level of command. Unimpeded access to all information, that is relevant to the decision-making issues of the moment, is the essential enabling function that permits timely and intelligent decision-making.

The basic goal of a Command and Control process is the *timely reduction of uncertainty to achieve intelligent decision-making*. *Sending orders and receiving reports are actions which directly result from the Command and Control process*.

Command Decisions

To win, a commander must gain the initiative and avoid being placed into a reactive mode by letting his opponent seize the initiative. To achieve that goal, the commander must operate "inside the decision loop of his opponent."[3] Therefore:

- The commander's command and control decision-making process, and the information systems that support that process, must be quick and agile;
- Actions also can be taken to impede his opponent's decision loop by injecting uncertainties that slow, deceive, or disrupt the opponent's process.

The need to operate inside the opponent's decision loop relates to all three types of command decisions:

a. Informational Decisions ("What is the situation?");

b. Organizational Decisions ("How to organize to achieve goals?");

c. Operational Decisions ("What actions should be taken?").

"Operational decisions" (about the actions to be taken by subordinate commanders) are always preceded by "informational decisions" (about what is happening.)

Information Support

To be responsive to the full range of decision-making, I believe that a Command and Control Information System must include two modes of operation:

- "Information Push," wherein pre-defined data and information products are provided to the decision-maker, or supporting staff, automatically by the system. These might take the form of reports or situation data derived from a pre-defined set of databases or threshold type reports;
- "Information Pull," wherein the decision-maker, or supporting staff, obtains desired data or information products by accessing local or remote databases, interactively, through use of appropriate search engines in order to obtain the inputs considered by the decision-maker or analyst to be necessary for the decision issue being addressed.

Informational Decisions

Informational decisions, either implicit or explicit, always precede the other two types of command decisions. Situation assessment is the general term. Prior to making an operational decision on the actions to be taken, a commander must decide what is actually happening, and what course the events are taking. These critical decisions are actually made on the basis of what the Commander believes is happening. The key issue, in both combat and crisis situations, is whether or not the Commander believes the strength, objectives, or rules of engagement of the enemy have changed to a degree that makes it necessary to change his prior assessment, and perhaps even his previously adopted operational plan.

Much of the information that a commander relies upon for decision-making is provided by his specialist staffs based on their assigned staff missions or specific tasks issued by the commander or his command group.

Intelligence is a good example of a functional area staff information product. In the case of the intelligence process, information rarely moves in its raw state directly from the sensor to the commander. Intelligence data not only passes through the links of a reporting system, it is also processed at intelligence nodes. This processing typically includes filtering, fusion, correlation, and analysis. Informational products provided by the other functional staffs, such as Operations, Logistics, CIMIC, and CIS also result from staff work carried out within a functional staff area; each product is also subject to similar processing actions.

Due to the importance of informational decisions, and the associated need for staff development of specialist inputs, a Command and Control Information System must include specific provisions for the accomplishment of this specialist work, and for the timely and accurate dissemination of the resultant information products. The System must make these products available to those, both local and distant, who are associated with the command and control process and who might have a need for them. The facilities that support specialist staff work are organized under the "Functional Area Subsystems" of the Command and Control Information System.

Organizational Decisions

The objective of "organizational decisions" is to achieve Unity of Effort in the pursuit of action through the establishment of a chain of command for an operation, definition of the lines of authority and responsibility, establishment of the flows of information, and identification of which commanders can make what decisions. Organizational decisions, made by the commander, are based on inputs obtained from subordinate commanders and specialist staffs. Since the proposed command decisions are normally developed under coordination by the command group and, when made, issued as orders by the Commander, support for these processes, and the rapid and effective promulgation of the resultant decisions, are important requirements to be met by a Command and Control Information System.

Operational Decisions

Operational decisions are the decisions made by a Commander when identifying the actions that are to be taken by his subordinate forces, based on his assessment of which course of action is the most effective one to pursue to achieve a mission. In addition to uncertainties about the situation and the course of action the opponent is about to select, operational decisions must be made in the face of uncertainties about the outcomes that would result from the interactions between the courses of action available to the commander and those available to his opponent. As an added complication, these interactions are influenced by decisions taken by a number of subordinate commanders on both sides. Operational decisions are also constrained by limits placed on the use of force imposed by the Rules of Engagement that are set by higher authority. Operational decision-making is complex, and made very difficult by the enormity of the potential outcomes that could result from the decisions made.

Operational decisions are made within the framework of a military planning process, which includes:

- "Development of the Commander’s Estimate of the Situation" (an informational decision necessary to choose a course of action);

- "Development of a Plan to Execute the Selected Course of Action" (a set of decisions which establishes the organization that is to execute the selected course of action, and defines the tasks to be accomplished by each of its component elements);
- "Promulgation of a Directive/Order" (orders and allocation of the authority to execute the Plan); and
- "Supervision of the Planned Action" (monitoring progress made to determine if changes in the Order, issued for the Plan, are necessary to accomplish the mission).

When making the fundamental operational decision as to the Course of Action to select, alternatives must be postulated and analyzed to assess:

- Suitability: "Will successful execution result in mission accomplishment?"
- Feasibility: "Can the potential course of action be accomplished with the means available?"; "Is the potential course of action consistent with the Rules of Engagement?"; "Does the potential course of action take into account the opposition expected?"
- Acceptability: "Do costs (losses) exceed the value of the objective achieved?"

Since the Command and Control process must enable the commander to operate inside the decision loop of his opponent, while at the same time providing for the timely reduction of uncertainty to support intelligent decision-making, an effective Command and Control Information System is one that includes embedded Decision Support Tools designed to assist in assessing the suitability, feasibility, and acceptability of the potential courses of action. The primary objective of these Decision Support Tools should be to provide insights into the probable consequences of the alternative courses of action, by predicting the probable outcomes of the possible interactions among the courses of action that might be selected by the Commander and his opponent.

Required System to Support Command and Control

The primary elements of a Command and Control Information System are:

- Communications Network: A responsive and secure communications network, to link the military headquarters across all levels of command (National, Strategic, Operational, and Tactical), is the essential capability which enables the National Command Authority, and its associated chain of command, to effectively control all national military forces in the application of military power to achieve national objectives. The communications network must provide for the timely transmission of orders and directives from higher headquarters to all subordinate forces, and the timely receipt of reports, from all subordinate headquarters of the constituted military force structure. This capability enables the empowered headquarters, in the chain of command, to monitor and control the authorized military operations. Both secure voice service and secure data transmission capabilities are required.
- Headquarters Information System: An information system is required at each command headquarters to provide timely and effective analytic support to the commander, and his specialist functional area staffs, to enable the commander to issue orders and directives that are both timely and based on a process designed to reduce uncertainty and enable intelligent decision-making across the entire spectrum of "informational," "organizational," and "operational" decisions. This requires information subsystems, organized along functional area specialist lines, that include the databases and decision support tools necessary to enable the specialist staffs to accomplish their work in a timely and competent manner.

A Network Architecture for Bulgarian Command and Control

A network structure for Bulgarian Command and Control could be as illustrated below:

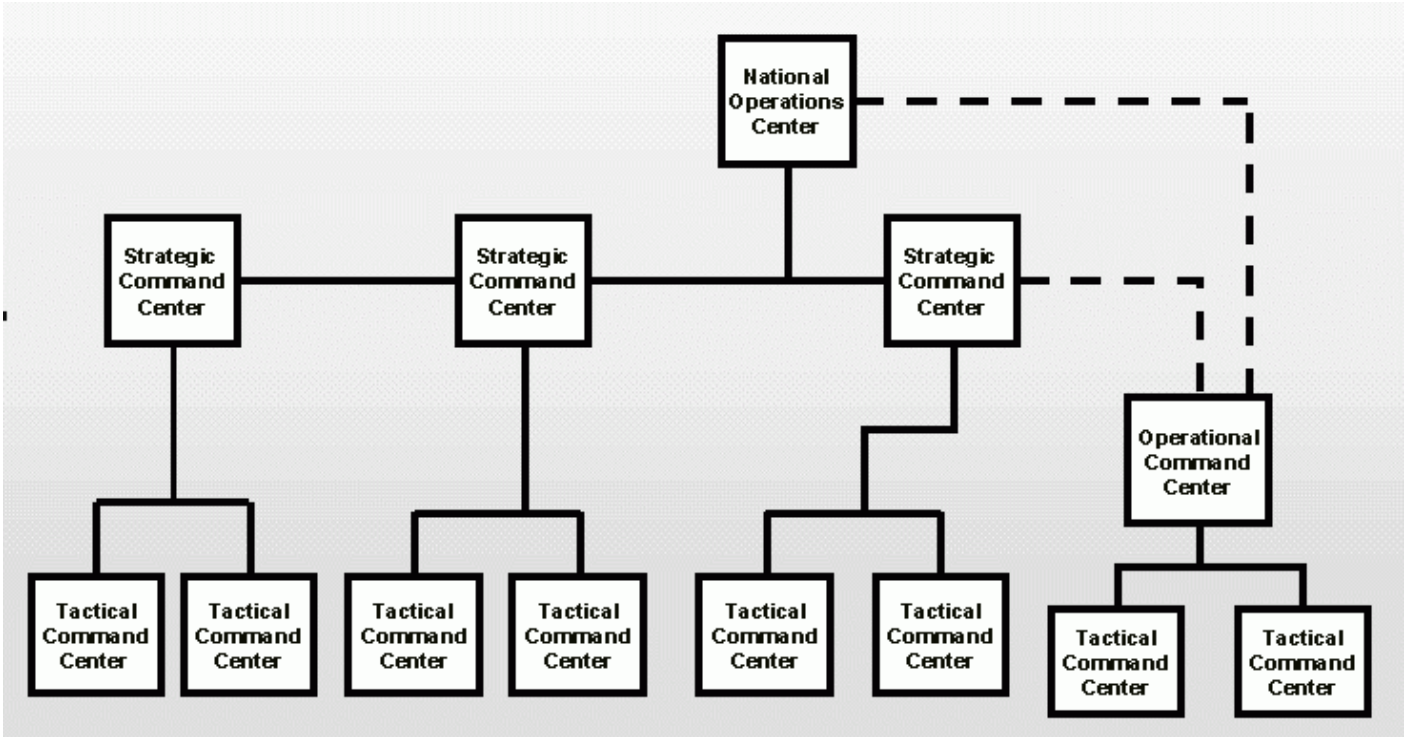


Figure 1: Network Structure for Bulgarian Command and Control

The Bulgarian command levels could be defined as follows:

- National: Chief of the Bulgarian General Staff, operating under the authority and direction of the National Command Authority;
- Strategic: Commanders of the Bulgarian Land Forces, the Bulgarian Air Forces, and the Bulgarian Naval Forces;
- Operational: Commander of an appropriate Strategic Command, or Commander of the Rapid Reaction Corps; designated on a case by case basis by the Chief of the General Staff;
- Tactical: Commanders of Rapid Reaction Corps, 1 Army Corps, 3 Army Corps extending down to the Commanders of subordinate Brigades; Commanders of Tactical Aviation Corps and Air Defense Corps extending down to the Commanders of subordinate units considered equivalent to Brigades; Commanders of Varna and Bourgas Naval Bases extending down to the Commanders of subordinate units considered equivalent to Brigades.

In this construction, it is assumed that the role of an Operational Headquarters, should one be required for a particular operation, would be assigned either to one of the Strategic Commands or to the Rapid Reaction Corps. The need for a deployable Command Center to support an Operational Headquarters, as is the case for a NATO Combined Joint Task Force (CJTF) Headquarters, should be considered.

Generic Command and Control Node

From an architectural point of view, a Command and Control Node can be considered to comprise the following major generic elements:

- Common System Services Element,
- Functional Area Software Support Subsystems Element,
- Operations Center Element.

Each of these elements can be defined in terms of both structure and capabilities.

C2 Node (Common System Services Element)

Each node of a Command and Control System should include the capability to provide common system services in support of the Commander and all functional area subsystems associated with the Command Center. These Common System Services should include: access to the external wide area communications network, electronic mail, messaging, file exchange, command briefing support, functional area database servers, geographic information services, information management (archival, documents, bulletins), information security (system access, firewalls, and guards), and technical support for local and distributed training and exercises, e.g., Computer Assisted Exercises.

Structurally, the common system services would be obtained by the users through Servers, accessed over a Local Area Network as illustrated in the Figure 2.

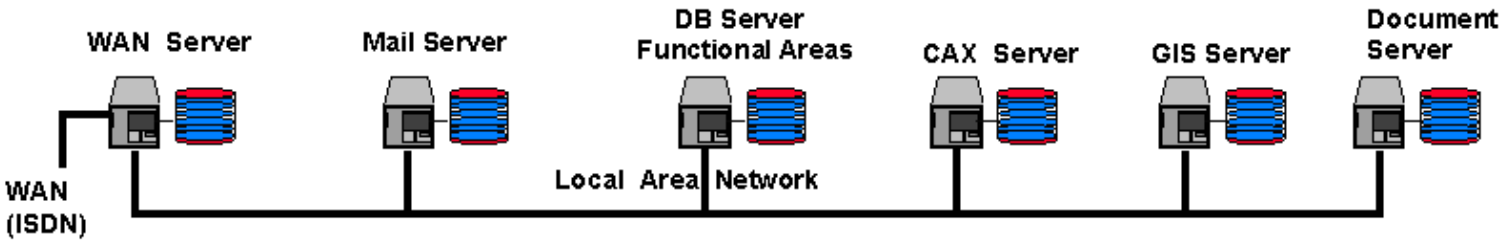


Figure 2: Generic C2 Nodal Architecture (Common System Services Element)

These common system services, on their own, provide a very effective level of technical support for Command and Control, if provided in a TCP/IP router-based sub-network, and if implemented at each Command Center in the chain of command. With such capabilities, the Commanders are linked through a secure data network that enables secure and timely dissemination of Orders and Directives to all subordinate commands, upward transmission of Reports from all subordinate commands, and lateral coordination among the commands at all levels. Staff work at each command would be facilitated through the provision of a standard set of briefing support packages that are compatible throughout the chain of command, thereby permitting analyses and briefings to be assembled using inputs provided directly by dispersed subordinate units. A common geographic information service implemented throughout the chain of command, would ensure consistent mapping as well as timely and accurate location information.

These Common System Services, resident at each Command Center, provide an essential foundation for subsequent expansion of the System through the addition, on an incremental and evolutionary basis, of the Operations Center capabilities and the Functional Area Software Support Subsystems.

C2 Node (Functional Area Software Support Subsystems Element)

A Command and Control Information System should be organized to accommodate the specific decision support requirements placed on the specialist staffs assigned to each command headquarters. This orientation permits each C2 Functional Area Subsystem to be designed to respond to specific functional staff requirements. This subsystem orientation is also consistent with the Command and Control Information System structure chosen by NATO. Adoption of this approach by Bulgaria would not only facilitate interoperation with NATO systems but also would enable Bulgarian personnel to gain experience in headquarters operations that would prepare them for future assignments, either in a Combined Joint Task Force (CJTF) Headquarters of a NATO-led Peace Support Operation, or ultimately in a NATO military headquarters such as SHAPE or Regional Command South.

This element of the Command and Control Information System would be organized to include Functional Area Staff Subsystems for Personnel (J1), Intelligence (J2), Operations (J3), Logistics (J4), Operations Analysis and Planning (J5), CIS (J6), CIMIC (J9), Engineers, and Weather (see figure 3).

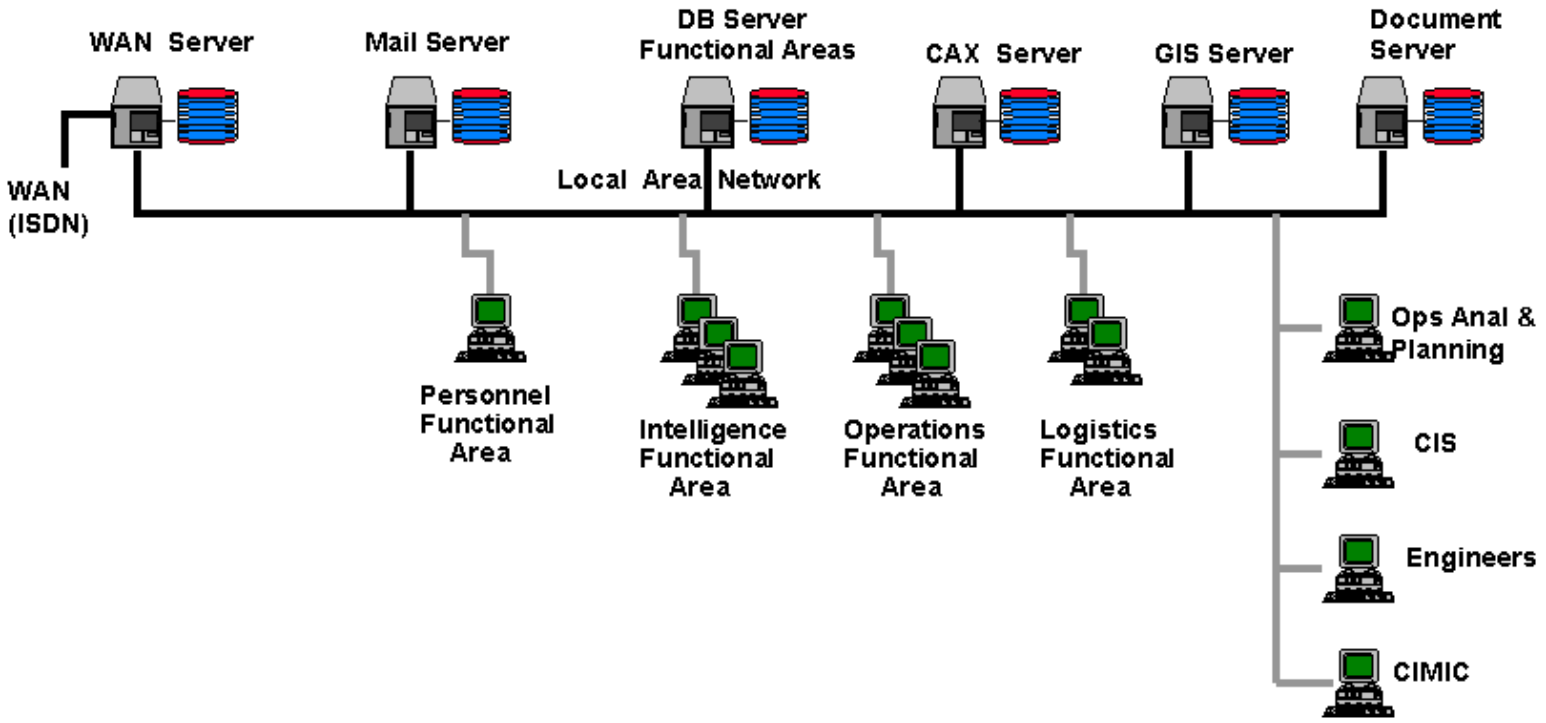


Figure 3: Generic C2 Nodal Architecture (Add: Functional Area Software Support Subsystems Element)

Key capabilities would include:

a. Production of specialist staff inputs for command decision-making;

b. Support for the effective management of the specialist staff work;

c. Development and maintenance of the functional area databases;

d. Reach-back access to databases held at other commands;

e. Interfaces with databases held by other functional area staffs;

f. Employment of appropriate Decision Support Tools;

g. Promulgation of orders and tasks to local and dispersed subordinates, assigned to work in the specialist functional staff served by the subsystem;

h. Response to imposed orders, tasks, and process requirements;

i. Production of data and information for consumption by other local and distant functional area subsystems;

j. Response to local and remote requests for expert data and assessments.

Structurally, the functional area software support capabilities would be implemented at each Command and Control Node through one or more staff workstations, that access the common system services and exchange information with each other over Local Area Networks as illustrated in Figure 3. The servers for the functional area databases would be associated with the common system services element to facilitate access from other Command and Control Nodes and from other functional staff elements within the command headquarters.

C2 Node (Operations Center Element)

The Operations Center Element, of the Command and Control Node, provides the facilities used by the commander's headquarters staff to support the work of the Commander in reaching his "informational," "organizational," and "operational" decisions.

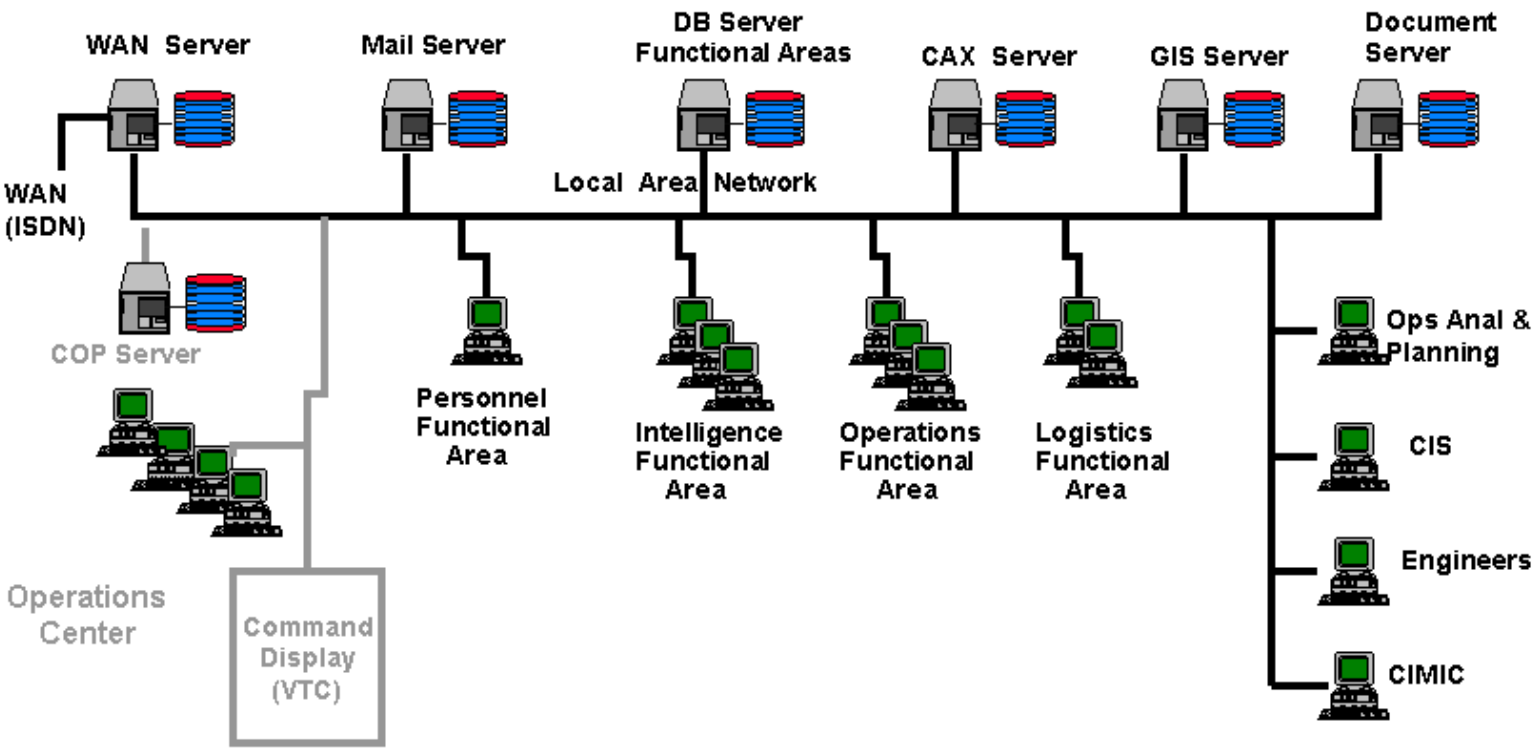


Figure 4: Generic C2 Nodal Architecture (Add: Operations Center Core)

The major capabilities would include:

a. Coordination of the staff work carried out by the functional area staffs of the headquarters;

b. Analysis and coordination of Course of Action alternatives;

c. Development of coordinated Staff Recommendations for consideration by the Commander;

d. Construction and maintenance of the Common Operational Picture held by the Command, integrating information provided by the functional area staffs;

e. Employment of appropriate Decision Support Tools;

f. Coordination of Command Decision Briefings;

g. Promulgation of Command Decisions and Directives;

h. Management of the Commander's Decision Briefings and Conferences.

As indicated on Figure 4, these functions would be accomplished through staff workstations and a Common Operational Picture (COP) server that access the facilities of the common system services element via Local Area Networks, a video-teleconferencing center, and a command center display facility. The video-teleconferencing and command center display facilities would be designed to interoperate with like facilities employed in the other Command and Control Nodes of the network. It is highly desirable that the video-teleconferencing and command center display facilities be compatible with those used by NATO, to facilitate Bulgarian participation in NATO-led Peace Support Operations, or ultimately in NATO collective defense activities.

Components of a Command and Control System

The main C2 system components, that emerge from the analysis of its operational requirements and structure, include: Personnel; Processes and Procedures; Data and Information Processing Equipment comprising local databases (structured and unstructured), access to local and remote databases (structured and unstructured), local analytic and decision support tools, and collaboration tools (local and remote participants); Displays; Communications Equipment comprising TCP/IP routers, local area networks, access to wide area networks, and video teleconferencing facilities; Electronic Support Means such as sensors and electronic warfare elements; and Access to Common System Services.

Architectures

To provide a foundation for the design, development, and implementation of a Command and Control Information System, three types of architectures are generally developed; namely, an "Operational Architecture," a "System Architecture," and a "Technical Architecture." When developing these architectures, it must be kept in mind that architectures are only a means to an end, not ends unto themselves! Accordingly, each architecture document should be minimum in depth, maintain some flexibility, and considered a "living document" so changes can be incorporated as requirements, threats, or technology evolve.

Operational Architecture

The purpose of an Operational Architecture is to identify the principal organizations that are to be served by the Command and Control System, the functions of the participating organizations, the inter-relationships among the organizations, the basic functional composition of the system, the general types of information to be exchanged in the system, and the primary external system interfaces that must be accommodated. Since the Operational Architecture provides a simple description of the primary operational requirements for the system, the main points to be addressed for a Bulgarian C2 System should include:

a. Organizations Served: Confirmation that the chain of command consists of four levels as described, and the identification of the Bulgarian commands at each level; confirmation that the tactical structure to be served includes organizations of Brigade size and larger; clarification of the Operational Level of command, and the need for a deployable Command Center for that level; and the identification of the functional staff organization at each command level.

b. Functions of System: Statement of the basic functions to be supported by the system (e.g., the need to support the command's informational, organizational, and operational decision-making); the need to provide easily accessible network-wide databases; and the need to provide appropriate Decision Support Tools for each functional area subsystem.

c. Operations Center oriented System Nodes: Statement of the need for "Operations Center" oriented Nodes having both Joint and Single Service configurations; requirements to support Command decision-making and promulgation of Orders and Directives; requirement to provide distributed Briefing and Information Support; need for a design which is Staff Cell driven; and the need for interoperability with National, Regional, and NATO Commands.

d. Modes of Information Transfer: Types of traffic required (voice, data, e-mail, video-teleconferencing); identification of the Command levels at which video-teleconferencing is required; requirement to provide reach-back capabilities (intelligence support, logistics, personnel, troop morale) to minimize the need for forward deployed databases; and the security requirements of the system.

e. System Flexible in Configuration and Use: Definition of capability for use at the National, Strategic, Operational, and Tactical levels of command; capability for use in National, Regional, and NATO-led Military Operations; capability for use in Combat, Peace Support, and Humanitarian Relief Operations; capability to accommodate tactical levels from Corps to Brigade; and need for components which are dismountable for use in buildings of opportunity.

System Architecture

The purpose of the System Architecture is to identify the form of the system, to identify the subsystems that will be used to implement the system and to fulfill the system requirements, and to allocate performance and functional requirements to the associated subsystems. The main points to be addressed should include:

a. Identification of System Structure: Establishment of the scope of the system; definition of the operational capabilities to be provided; and specification of the end-to-end performance requirements of the system.

b. Identification and Definition of Subsystems: Identification of the operational drivers for the subsystem definitions; alignment of the subsystems with the Command and Control Process; and the identification of the participants in subsystem processes.

c. Allocation of Functions to Subsystems: Derivation of the required subsystem functions from the defined system capabilities; identification of the basic subsystem inputs and outputs; and the specification of the performance requirements to be satisfied.

Technical Architecture

The purpose of the Technical Architecture is to identify the technology and technical standards to be applied to the design and implementation of the system. This need not be an extensive elaboration of all matters; of most importance is that the essential or critical technical standards be identified. The Technical Architecture should address: requirements for application of ISO/OSI Open System Standards (NATO Compatible); use of Client-Server networking; incorporation of web-enabled database access software; employment of a Geographical Information System which complies with NATO standards; establishment of a TCP/IP router-based data sub-network; provision of access to Wide Area Networks, including strategic communications networks based on ISDN standards and tactical communications networks based on Eurocom D/1 standards; adoption of video-teleconferencing standards compliant with those of NATO; establishment of a strategy calling for maximum use of Commercial-Off-The-Shelf products, with designation of preferred products; and definition of feasible INFOSEC concepts.

Command and Control System (Development and Acquisition)

Since a Command and Control System must support complex, multi-echelon, command decision-making, it is virtually impossible to build a Command and Control System as a "turn-key" solution. To succeed in implementing this class of system there must be close and continuing interactions throughout the development process with the user community, and with senior commanders and their functional area staffs in particular.

Experience indicates that the most successful development and implementation paradigm for a Command and Control System is one that incorporates an *Evolutionary Development and Acquisition approach*, which is firmly based on a program of User-Oriented Prototyping and Testbedding to capture the operational requirements and to provide proof of concept prototype solutions, suitable for evaluation, prior to any large commitment of money for the implementation phase. Cost and performance risks are minimized by involving the user, at the earliest possible time, in the translation of operational requirements into system solutions and by the evaluation of prototyped proof of concept implementations.

Evolutionary Development and Acquisition also provides an ability to time phase the implementation of a System in a manner consistent with the availability of procurement funds, an ability to easily respond to the identification of new or revised operational requirements necessitated by changes in operational concept, threat, or technology, and an ability to continually exploit emerging technology in order to implement new operational capabilities.

With the Evolutionary Acquisition paradigm, a Command and Control Information System is implemented in an incremental manner. Increments are designed either to add a new capability to the system, to increase the capacity or scope of the system, to infuse new technology to reduce costs, or to obtain a capability that previously had not been feasible due to technology limitations. The initial core capability of the system and all incremental enhancements to the system are formulated in compliance with the operational, system, and technical architectures established for the system.

Under the concept of User-Oriented Prototyping and Testbedding, both the application of commercial products and the development of all functional area software support subsystems and their associated decision support tools, follow a development and acquisition path that involves laboratory prototyping to technically determine the optimum method for implementing, or integrating, a desired new capability into the Command and Control System as it exists at the time.

When all technical issues are resolved, the prototyped capability is integrated into a laboratory testbed to obtain informal user reaction; if found to be of apparent operational value, the capability is then implemented in a system model, maintained by a Bulgarian Technical Center, which

faithfully emulates the fielded Command and Control System, for the purpose of obtaining a more complete user evaluation of the proposed incremental capability. Operational personnel, assigned to a Command Center, would carry out this user evaluation. If the user evaluation is favorable, a proposal will be prepared, for approval by appropriate Bulgarian authorities, to acquire the capability for integration into the operational Bulgarian Command and Control System. A field evaluation would then be conducted at one or more of the implementation sites to confirm user acceptance.

As can be seen, the steps of the process significantly reduce not only the cost risk but also the risk associated with ultimate user acceptance of the fielded product. The process ensures effective technical integration into the fielded System. It also produces sound data to support acquisition decisions by the procurement authorities since technical feasibility would have been demonstrated, the operational acceptability of the proposal would have been confirmed by the users, and reliable cost figures would be available.

Another attribute of the process is its inherent compatibility with the strategy of maximizing the use of commercial off-the-shelf products and the objectives of maximizing national content and maintaining firm control of the development and acquisition process.

Recommended Incremental Strategy for C2 System Implementation

The following incremental strategy for implementing the Bulgarian Command and Control System is recommended:

a. Step 1: Establish the basic router-based communications infrastructure and implement an initial core system capability by prototyping, evaluating and acquiring the Common System Services Element of the C2 System, as defined above and illustrated in the Figure 2, but with the following initial modifications:

(1) Delay implementation of the Functional Area Database Servers;

(2) Delay implementation of the CAX Servers;

(3) Provide two or three workstations as an initial capability for accomplishing the work of a Command Center, to provide messaging capabilities that include electronic mail, and to implement effective capabilities for transmission of Orders and Directives from higher headquarters, and receipt of Reports from subordinate headquarters.

This initial capability should be implemented at all Command and Control Nodes, thereby linking all headquarters of the military chain of command to provide the essential communications and information system support needed for combat, peace support, and civil crisis operations. Even in its initial form, the establishment of such a secure and responsive C2 Network, linking all national forces with their National Command Authority, would be viewed as very significant with regard to NATO preparation.

b. Step 2: Define, develop, prototype, evaluate, and acquire the three functional area databases considered of most importance to support the work of the Intelligence and Operations staffs of a Command Center. Tailor these capabilities as appropriate for the level of command at which they are to be implemented. Also, acquire the staff workstations and necessary Local Area Network capabilities to connect these two functional staffs into the Command Center, as illustrated in the Figure 3. Provide functional area database servers and integrate the acquired capabilities into the Command Centers of the System.

c. Step 3: Define, develop, prototype, evaluate, and acquire the three most important capabilities required to implement the Operations Center Element of the Command and Control System, as described above and illustrated in the Figure 4. These capabilities should be tailored, as appropriate, for the level of command at which they are to be implemented.

d. Remaining Steps: Similarly defined follow-on incremental steps for the continued evolution of the Bulgarian Command and Control System should be formulated in conjunction with the General Staff. These follow-on steps should provide for the definition, development, prototyping, evaluation, and acquisition of the additional capabilities needed to evolve the capabilities of the system, to develop the databases needed by the remaining functional area staffs, to implement the necessary decision support tools for all functional subsystems, to enhance the capabilities of all functional area software support subsystems, to implement web based database access capabilities to support access by personnel of other functional areas and other operational commands, to complete the capabilities of the Operations Center Element, and to generally expand the system capabilities in response to user requests.

Conclusions

This Paper has provided an examination of the accepted definition of "Command and Control," and from that examination derived the fundamental operational requirements for a Command and Control Information System, outlined the operational, system, and technical architectures for that system, and put forward a basis which can serve as the foundation for the evolutionary implementation of a Command and Control capability that extends across all levels of command to include National, Strategic, Operational, and Tactical requirements.

Employment of an evolutionary development and acquisition paradigm for implementing the required C2 capabilities is recommended because it not only minimizes operational and technical risks but also ensures that an effective core system capability is realized in a timely manner, while establishing a sound basis for the follow-on enhancement of that capability at a rate commensurate with the availability of the necessary additional funding. User oriented prototyping and testbedding should be a part of that process to ensure active user involvement, supported by

proof of concept prototyping, thereby ensuring user acceptability of the developed capabilities and the reduction of cost risk.

References:

1. Frank M. Snyder, *Command and Control: The Literature and Commentaries* (Washington, DC: National Defense University, 1993). Further readings include Kenneth Allard, Command, Control, and the Common Defense, revised edition (Washington, DC: National Defense University, 1996); David S. Alberts and Richard E. Hayes, *Command Arrangements for Peace Operations* (Washington, DC: National Defense University, 1995). The latter books are available in electronic at http://www.ndu.edu/inss/books/

2. Jon L. Boyes and Stephen J. Andriole, eds., *Principles of Command and Control*, Foreword by Gen. Russell E. Dougherty (Fairfax, VA: AFCEA International Press, 1987)

3. John R. Boyd, *A Discourse on Winning and Losing* (Maxwell AFB, Alabama, 1987).

LOREN DIEDRICHSEN has a BS in Electrical Engineering from Iowa State University and an MS in Operations Research from the Stevens Institute of Technology. He is now a Defense Consultant, after having completed 14 years as a member of the NATO International Staff, serving as Principal Technical Advisor in the NATO CIS Agency, Director of the SHAPE Technical Centre, and the first General Manager of the NATO C3 Agency. Prior to joining NATO, he was employed for 27 years in various research, development, and acquisition posts of the US Army including Chief of System Engineering for the Joint TRI-TAC Program and Director of the US Army Center for System Engineering and Integration. He is a Senior Member of the IEEE, and a Distinguished Life Member of AFCEA.

BACK TO TOP

Information & Security. An International Journal
e-mail: infosec@mbox.digsys.bg

Command & Control: Operational Requirements and System Implementation

Loren Diedrichsen

Keywords: Command and control, operational, technical, system architectures, evolutionary development.

Abstract: This paper examines accepted definition of "Command and Control" (C2), and from that examination the author derives the fundamental operational requirements for a Command and Control Information System. The result is an outline of operational, system, and technical architectures for such a System, creating a basis for the evolutionary implementation of an effective Command and Control capability that extends over all levels of national command. The author recommends employment of an evolutionary development and acquisition paradigm for implementing the required C2 capabilities. Such approach not only minimizes operational and technical risks but also ensures that an effective core system capability is realized in a timely manner, while establishing a sound basis for the follow-on enhancement of that capability at a rate commensurate with the availability of the necessary additional funding. User oriented prototyping and testbedding should be a part of that process to ensure active user involvement, supported by proof of concept prototyping, thereby ensuring user acceptability of the developed capabilities and the reduction of cost risk.

Authors: **Stoyan Balabanov and Karmen Alexandrova**
Title: **C4I System Reengineering: Essential Component of Bulgarian Armed Forces Reform**
Year of issuance: **2000**
Issue: **Information & Security. Volume 5, 2000**
Hard copy: **ISSN 1311-1493**

C4I SYSTEM REENGINEERING:

ESSENTIAL COMPONENT OF BULGARIAN ARMED FORCES REFORM

Stoyan BALABANOV and Karmen ALEXANDROVA

Table Of Contents:

The principles and issues of establishing a modern, combat-ready and highly effective army, defined in the Military Doctrinaire of the Republic of Bulgaria, are based on the notion of the priority of the command, control, communications, computers and intelligence systems (C4I). C4I development must comply with current combat requirements of the armed forces, but also must guarantee compatibility with the armed forces of NATO member countries.[4,5,6,7] The modernization and implementation of new C4I systems are considered as top priorities in the Plan for Organizational Development and Structural Reform of the Armed Forces by the year 2004 ("Plan 2004").

Bearing in mind the importance of C4I systems and the need of clear strategy and long-term concept for their development, and in accordance with a resolution of the Council of Ministers, an extensive study was conducted in the MoD with the expert assistance of MITRE Corp. and the Electronic Systems Center of the US Air Force. The study was considered essential for Bulgaria's preparation to become a NATO member. It was carried out between July 1999 and January 2000. Experts from the Directorate of Communication and Information Systems of the General Staff (GS), the Defense Panning Directorate, the Institute for Advanced Defense Research (IADR), the Land Forces HQ, the Air Force HQ and the Navy HQ took part in it. The separate phases and some of the study outputs are shown on Figure 1.

The major objectives of this study were focused on achieving operational compatibility with the US and other NATO militaries. In order to achieve these objectives, conducted analyses and assessments of the current state of affairs and planned architectures in the field of C4I systems were taking into account the desired operational compatibility. Based on all that, the main recommendations and priorities for further development of C4I systems were defined.[2] In the course of the local study, carried out in July 1999, a number of Bulgarian and US experts produced and exchanged preliminary reports through briefings. In the conclusive stages of the study the American experts submitted an official Final report.[8]

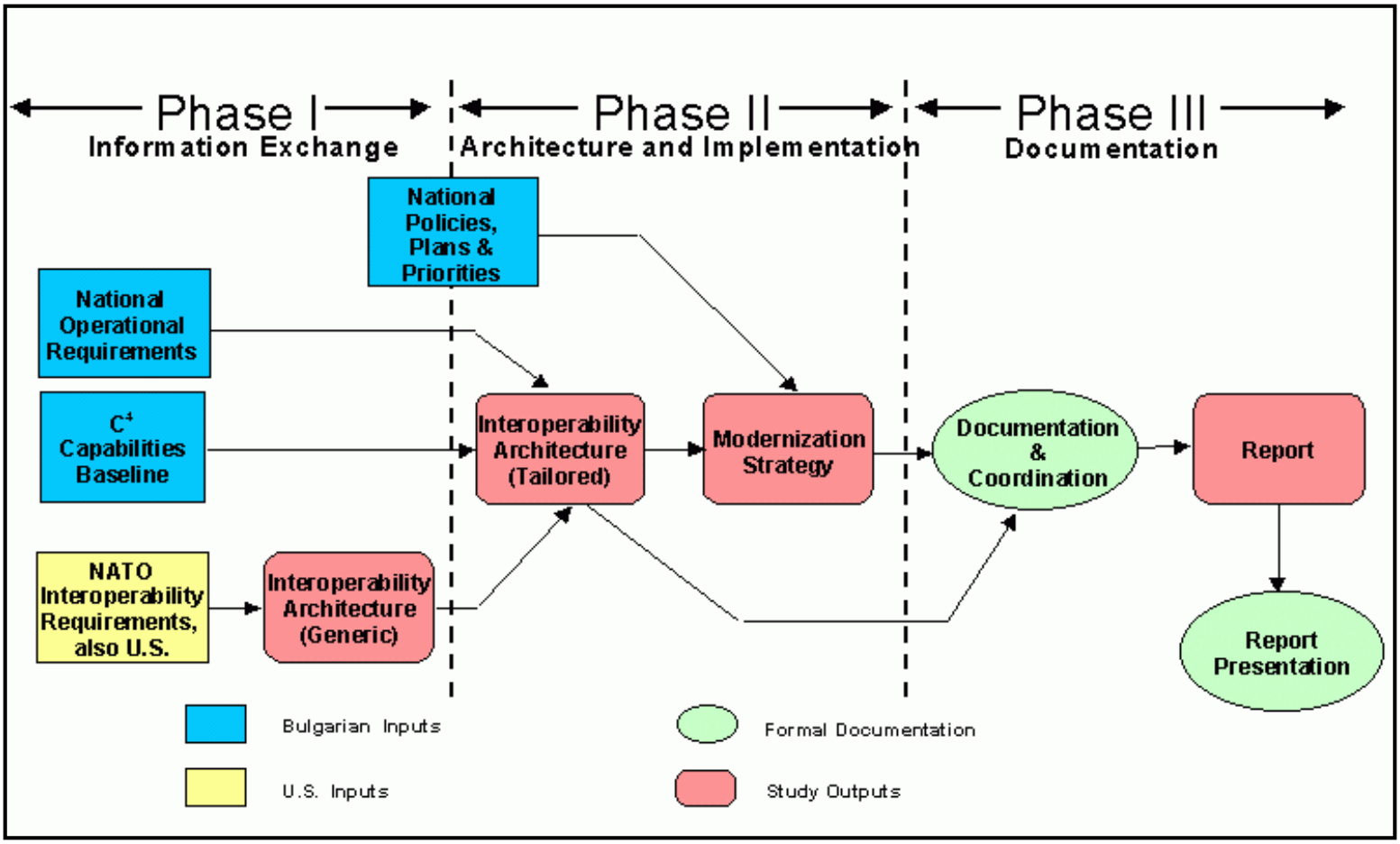


Figure 1. Functional Flow of C4I Study Process

This study proposed concrete and important steps towards improving:

- the life cycle of C4I systems;
- C4I planning and development strategy;
- the process of pinpointing the priority projects in the field;
- the mutual coordination, and
- the financing principles.

We can point out as major achievements the adopted:

- Manual for C4I Life Cycle Management in the Ministry of Defense and the Bulgarian Armed Forces (BAF) [3];
- Programming principles of administering and carrying out C4I projects by a program director and • program team;
- Institution of Chief information Manager of MoD

The final documents of the study [2,8] describe the architectures of compatible C4I systems that are operationally effective and economically acceptable for Bulgaria.

The results of the study are summarized as recommendations for modernizing C4I systems at different priority levels. The modernization programs and priorities are grouped in three categories according to how far our country has come in preparing for NATO membership.

Top priority are the requirements and activities considered as preparation for NATO membership.

Second priority are the requirements and activities for becoming a NATO member.

Third priority are the requirements and activities that we need to fulfill after becoming a NATO member.

This approach allows step-by-step allocation of financial resources and aims at achieving defined political objectives and carrying out the reform in the Bulgarian armed forces.

Few concrete activities, concerning special thematic fields and priorities were established taking into account the great importance of maintaining an effective defensive capability of the country:

- Command Staff Automated Management System (CS AMS) Integration;
- Air Defense Modernization;
- Field Integrated Communication and Information System (FICIS);
- South East Europe Brigade (SEEBRIG);
- Data Networks;
- Network and Systems Management (NMS);
- Computer-Assisted Exercises (CAX);
- Information Technology and Management;
- System Acquisition;
- Information Assurance (IA).

Achieving operational, system and technical compatibility

The following basic principles must be applied while designing and developing C4I systems in the Ministry of Defense (MoD) in order to achieve operational, system and technical compatibility among C4I systems of the Bulgarian army and those of NATO member countries:

- Develop unified peacetime/wartime information systems;
- Programming project implementation;
- Wide use of COTS technologies
- Satisfying all operational requirements
- Compatibility among the separate subsystems, national C4I systems and, if needed, with systems of NATO member or partner countries;
- Mobility (for the field systems);
- Survivability;
- Endurance – the ability to support all operations regardless of their duration;
- Reliable information protection on all levels according to the level of classification.

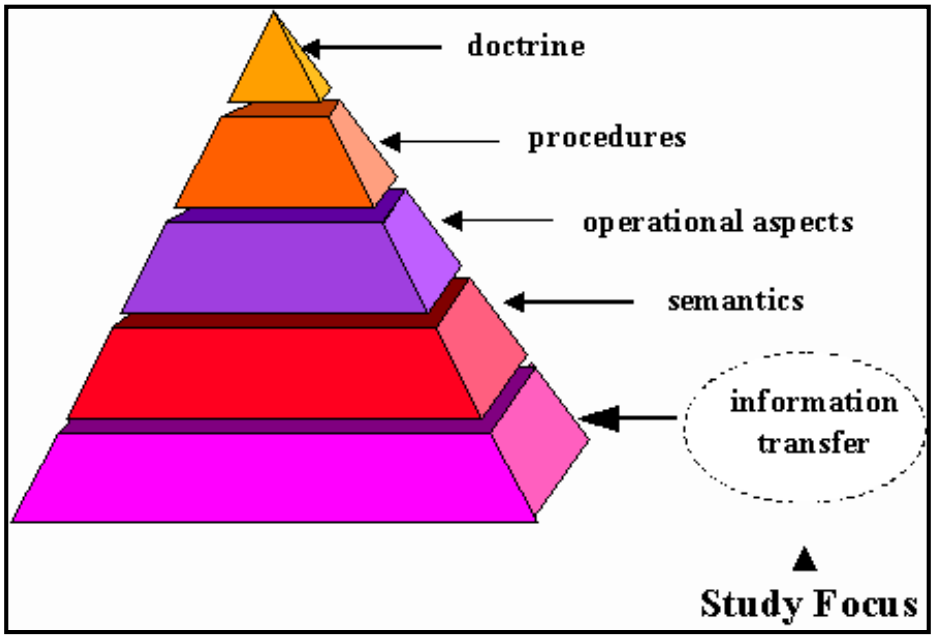


Figure 2. The Interoperability Pyramid

The operationally compatible architecture, presented in this report, describes how C4I systems of the Bulgarian armed forces can fulfill the recommended requirements for operational compatibility with the systems of NATO member countries and USA (Figure 2).

The focus of this architecture is on information transfer mechanisms and the types of information services supported over the suggested interconnections. Where possible, specific types of interfaces with NATO and U.S. systems as well as the standards that define the technical characteristics of the interfaces are recommended. The goal of the interoperability architecture is to achieve NATO level 4 interconnection among Bulgarian C4 systems and both NATO and U.S. C4 systems.

The key features and attributes of the architecture recommended for interoperability among Bulgarian C4 systems and NATO C4 systems are as follows:

- Voice and fax service (clear and secure) provided by an interconnection between the planned Bulgarian digital switched network and the NATO Core Network (NCN);
- Secure message service provided by an extension of the NATO X.400 and Simple Mail Transfer Protocol (SMTP) messaging system through the NATO Internet Protocol (IP) router network to Bulgarian X.400 and SMTP;
- Message transfer agent gateways;
- Air operations communication support provided by NATO’s tactical digital information data link extensions to Bulgarian entities and by exchange of formatted messages;
- Maritime operations communication support provided by NATO’s tactical digital information data link extensions to Bulgarian entities, by exchange of formatted messages and by configuring selected Bulgarian vessels to read the NATO Fleet Broadcast;
- Command and Control Information System (CCIS) information exchange provided by remote NATO CCIS terminals (using air gap interfaces), migrating to Bulgarian/NATO CCIS system interconnection through an approved Guard via the NATO IP router network;
- Unclassified electronic mail (e-mail) exchange provided by Transmission Control Protocol/Internet Protocol (TCP/IP)- Internet based connections, buffered through firewalls for security;
- Video teleconferencing services provided by dial-up Integrated Services Digital Network (ISDN) secure connections between Bulgarian and NATO 128 kbps Video Teleconferencing (VTC) systems (dual 64 kbps connections);
- Exchange of intelligence information, provided by a secure connection using web technology, between a Bulgarian system and an extension of NATO’s Battlefield Information Collection and Exploitation System (BICES) network;

- Extending Computer-Assisted Exercise's (CAX) capabilities from NATO to a Bulgarian CAX system using a NATO CCIS connection;
- Extending NATO's communication services to deployed Headquarters (HQ) provided by remote NATO systems initially, and subsequently migrating to Bulgarian/NATO system interconnections similar to those used in fixed systems;
- Tactical area network interconnections established in accordance with EUROCOM D/1 interface specifications for voice systems. IP router-based interfaces using Guard technology to support e-mail exchange, with migration to ISDN connections in the future are also proposed;
- Single channel radio system interoperability for all Bulgarian military services compatible with NATO single channel radio STANAGs;
- Common Combat Net Radios (CNRs) for Bulgarian forces participating in multinational operations;
- Identification Friend or Foe/Selective Identification Feature (IFF/SIF) interoperability by implementing NATO-compatible interrogator sets and transponders and also Mode S Transponders compatible with ICAO, Annex 10;
- Finally, a comprehensive system security infrastructure that is fundamental to the interoperability architecture.

The issue of the interoperability among Bulgarian and U.S. C4 systems arises in the context of the two nations participating in a bilateral or multilateral military operation outside the scope of a NATO operation. There is no current agreement between Bulgaria and the U.S. for such an operation. Consequently, the interoperability requirements and architecture configurations presented in this report are notional ones. In the event that Bulgaria and the U.S. agree to such an operation, both nations would identify appropriate military command authorities to establish specific operational agreements and information exchange requirements. One key purpose of discussing a potential interoperability architecture among Bulgarian and U.S. C4 systems was to illuminate the numerous areas in which NATO interoperability and U.S. interoperability are the same, or nearly so, and to point out the few areas in which they differ.

The key features and attributes of the architecture for interoperability between Bulgarian C4 systems and U.S. C4 systems are as follows:

- Voice and fax service (clear and secure) provided by interconnection between the planned Bulgarian digital switched network and the Public Switched Telephone Network (PSTN);
- Secure message service provided by an extension of U.S. Defense Messaging System (DMS) (X.400 and SMTP gateways) through a leased digital connection to Bulgarian X.400 and SMTP gateways;
- Air operations communication support provided by U.S. tactical digital information data link extensions to Bulgarian entities and by exchange of formatted messages;
- Maritime operations communications support provided by U.S. tactical digital information data link extensions to Bulgarian entities and by exchange of formatted messages;
- CCIS information exchanges provided by remote U.S. Global Command and Control System (GCCS) coalition terminals or Local Area Networks (LANs) (air gap interface to Bulgarian system), migrating to Bulgarian/U.S. GCCS coalition system interconnection through an approved Guard;
- Unclassified e-mail exchange provided by TCP/IP-based Internet connections, buffered through firewalls for security;
- Video teleconferencing services provided by dial-up ISDN secure connections between Bulgarian and U.S. 128 kbps VTC systems;
- Exchange of intelligence information provided by mutual U.S. and Bulgarian gateways into the NATO BICES network;
- Tactical area network interconnections established per EUROCOM D/1 specifications. If required, separate IP router-based interfaces using Guard technology to support e-mail exchange, with migration to ISDN connections in the future are proposed;
- Use of U.S. CNRs for Bulgarian forces participating in multinational operations with U.S. forces;
- Finally, the same comprehensive system security infrastructure that is fundamental to NATO's interoperability architecture.

It would take many years and considerable amount of resources to implement all the features and attributes identified above. Consequently, a subset of capabilities implemented over time appear to offer particular advantages in operational utility and technical implementation feasibility. It is assumed that implementation actions for achieving NATO interoperability will, in most cases, lay the foundations for Bulgaria/U.S. C4 system interoperability when required.

Recommendations for modernizing C4I systems and priority projects

The study addressed several additional C4 topics, among them Automated Management System Integration, Air Defense Modernization, Field Integrated Communication and Information System (FICIS), South East Europe Brigade (SEEBRIG) communications and information services, Data Networks, Network and Systems Management, Computer-Assisted Exercise, Collaborative Technologies, Information Technology and Management, System Acquisition and Information Assurance. These topics are vital, although not directly related to interoperability between Bulgarian and NATO/U.S. C4 systems. For these topics, the recommended actions are independent from future NATO accession dates and, in some cases, are separated into short-term actions (up to 2 years) and long term actions (more than 2 years). The implementation prioritization of these recommendations is as follows:

CS AMS Integration

The recommendations for the CS Automated Management System Integration are not divided into time categories. These actions should be accomplished to support the integration of the CS AMS:

- Prioritize requirements and subsystems in order to be integrated in the AMS;
- Provide clear definition of the requirements for each subsystem;
- Document AMS interfaces to other systems of the Bulgarian armed forces;
- Assess the expandability of the logistics system currently developed under the bilateral security assistance program ;
- Define the security concept;
- Involve experts with relevant experience.

FICIS

FICIS and security capabilities appear to meet short-term needs for tactical area systems. However, additional capabilities will be needed over time. Actions to support these capabilities include:

- Developing tactical area network architecture, including a clear definition of external system interfaces;
- Preparing a Concept of Operations (CONOPS) for the tactical area CIS;
- Formulating a migration plan to guide the evolution of the FICIS.

SEEBRIG

SEEBRIG communications and information system capabilities also appear adequate for short-term needs. To support the additional capabilities that will be needed over time, the Bulgarian armed forces should perform the following actions:

- Develop a CONOPS for SEEBRIG operations;
- Develop detailed CIS functional requirements. In addition, the BAF should consider FICIS functional capabilities needed for tactical units;
- Develop a system migration plan for CIS. This should include how the communications capabilities (SATCOM, replacement of Russian radios, common CNR, etc.) will be expanded, as well as how the office automation baseline will be enhanced with C2. While developing this plan, the BAF should consider INFOSEC implications ahead of time.

Data Networks

The following actions should be accomplished in the short term:

- Complete the planned network modernization at the MoD and extend this modernization to the Service HQs and lower echelons;
- Develop migration plans to guide the evolution of the Bulgarian defense LAN and Wide Area Network (WAN) infrastructures;
- Maintain cognizance of NATO network-related activities to facilitate future interoperability/compatibility efforts;
- Address issues regarding training and retention of skilled personnel to maximize benefit for the Bulgarian armed forces.

In the long term, the following actions should be accomplished:

- Evolve LAN and WAN infrastructures as per their respective migration plans.
- Develop an internal testbed to address both Information Technology (IT) and network interoperability issues and expedite future interoperability/ compatibility solutions.

While solving those problems, an important step forward is already being made. All requirements for establishing NATO and US LAN/WAN compatible networks are being noted and included in the technical requirements for the pilot project of Sofia's Garrison and the National Military Command Center.

Network and Systems Management (NSM)

For the short-term, it will be very important that the Bulgarian armed forces to prepare a concept of operations (CONOPS) for their NSM capabilities. In the long-term, the following should be accomplished:

- Define a NSM implementation for the BAF to include an organizational (e.g., hierarchical) and functional approach to the overall NSM process.
- Extend NSM to the service HQs and lower echelons.

CAX

The following should be accomplished in the short-term:

- Keep participating in Cooperative Automation seminar.

In the long-term, the following actions should be accomplished:

- Implement capabilities to participate in NATO CAX.
- Obtain JTLS [10] simulation model (or equivalent).
- Obtain releasable interface standards.

Information Technology and Management

For the short-term, the following should be accomplished:

- Continue the efforts to build the communications infrastructure that supports the expanded use of IT.
- Institutionalize the IT management process. This action would include the definition of a BAF IT vision; the selection of BAF hardware and software standards; and the institution of an Information Technology Steering Group (ITSG) to serve as the implementation mechanism for the activities. The focus of this effort is on the development of a Joint Technical Architecture/Common Standards Profile (JTA/CSP) and the selection of components for a Bulgarian COE.
- Develop an implementation strategy.
- Appoint an IT Steering Group to guide the implementation.

System Acquisition

The following should be accomplished:

- Ensure training and sustainment;
- Define a BAF C4 operational architecture;
- Assess how CIS capabilities support the operational architecture;
- Develop a CIS modernization roadmap;
- Support a phased, incremental implementation approach in accordance with BAF/MoD priorities;
- Revisit the operational architecture as missions evolve.

Information Assurance (IA)

The steps to be taken in the short-term in order to address information assurance requirements are as follows:

- Update security policies to cover the entire scope of IA;
- Review and update existing security organizational responsibilities;
- Establish new organizational entities as required;
- Establish an incident reporting and monitoring capability;
- Establish system high LANs and WANs;
- Develop and maintain comprehensive security architecture;
- Begin introduction of ‘protect, detect and react’ capabilities;
- Implement firewalls;
- Implement Intrusion Detection Systems (IDS) on critical LANs;
- Establish network scanning and vulnerability assessment;
- Develop an IA training and indoctrination program.

In the long-term, the following steps should be taken:

- Introduce application-specific Guards to interconnect system high networks;
- Provide an IA situation awareness capability in the NMCC and other operation centers;
- Develop and introduce an electronic key management system and Public Key Infrastructure (PKI).

Recommendations for the organizational structures related to systems development

Organizations

The following organizations in the Ministry of Defense and the General Staff support and develop C4I systems:

- Defense Planing Directorate;
- Institute for Advanced Defense Research (IADR) in the Defense College;
- Communications and Information Systems Directorate in the General Staff;
- Executive Agency "Central Military Support" (EA "CMS")
- Section "Information Support" in the Administration Support Directorate of the Ministry of Defense;
- "Information Support Center" in the General Staff;
- Program/project teams.

Defense Planning Directorate (DPD)

The main organization in the MoD that plans and organizes the activities related to the life cycle of C4I systems is the Defense Planning Directorate and its section "Programs for development of armaments, equipment and infrastructure". The directorate fulfills its functions in cooperation with all staff and non-staff bodies with responsibilities in regard to C4I system development and maintenance in the Bulgarian armed forces.

Institute for Advanced Defense Research (IADR) in the Defense College

The IADR is the main executive organization of the MoD in the field of forecasting, analysis, research, development, preparation of tactical-technical requirements, test and evaluation methodologies, methodologies for complex expert assessments, scientific-technical support of the research, testing and implementation of C4I systems. IADR researchers provide expert advice in all phases and stages of C4I acquisition process.

Communication and Information Systems Directorate in the General Staff (CISD-GS)

CISD-GS is responsible for the overall management and organization of the exploitation of C4I systems fielded by the Bulgarian armed forces. It takes part in the initial stage of a program/project by preparing initial requirements that define the operational system requirements, as well as in implementation and service testing of C4I systems.

Executive Agency "Central Military Support" (EA "CMS")

The executive agency is the main executive organ of the MoD that deals with commercial contracts, organizing service testing and implementing C4I systems and/or their elements (sub-products) and developing standardization documents and procedures for certifying producers of military and special products.

"Information Support" Section in MoD

The Section is involved in activities related to the development of initial requirements, implementation and maintenance of communications and information systems for the administration of the Ministry of Defense.

Information Support Center (ISC) - GS

The ISC is involved in activities related to the exploitation and maintenance of BAF systems. Occasionally, it may develop or adjust information systems on its own.

Program/Project Teams

For the realization and management of projects carried out by external contractors it is advisable to designate programming teams, managed by the Chief Information Officer and affiliated to IADR, Executive Agency "Central Military Support", or ISC – GH depending on the specific circumstances.

Other institutions

Among the consultative or managerial organizations with responsibilities for the management of C4I systems' life cycles, but have no permanent staff, are the following:

- Chief Information Officer;
- Programming Council of the Ministry of Defense;
- Expert Technical-Economic Council on C4I systems (ETEC on C4I)
- Scientific-Technical Commissions on C4I systems (STC on C4I)

Chief Information Officer

Major institution in the MoD that coordinates and oversees the activities related to the management of the life cycle of C4I systems,

as well as the coordination among various C4I system development programs, is the Chief Information Officer (CIO).

The responsibilities of the CIO are as follows:

(1) To advise and submit reports to the Minister of Defense and the senior management of the Ministry of Defense on issues related to information technologies and the management of information resources in order to ensure their competent use and implementation.

(2) To develop, maintain and facilitate the implementation of advanced information technologies and develop integrated information architecture of the Ministry of Defense.

(3) To ensure the effective design and operation of all major informational resources and processes in the Ministry of Defense.

(4) To manage the informational resources of the Ministry of Defense.

(5) To coordinate and control the main programs for developing the information technologies for the Ministry of Defense. To assess the course of these programs based on applicable funds for exercising control and advising the Minister of Defense in certain cases whether those programs/projects to be approved, modified or canceled.

(6) Annually, as a part of the strategic program planning and appraisal, to assess the defined requirements for MoD personnel related to their knowledge and skills of:

- managing and using informational resources;
- evaluating the information technologies proficiency of the different management levels in MoD;
- evaluating the level of conformity of the skills of the latter with the requirements for development of information technologies in MoD;
- If needed to initiate programs for personnel education and training.

(7) To report periodically to the Minister of Defense on the progress made while implementing information technologies in MoD

(8) In order to perform his or hers duties, the CIO prepares and submits for approval by the Minister of Defense:

1. Orders and suggestions for structural changes in the organizations supporting the development of information technologies in MoD.
2. Strategies and doctrines for implementing and developing information technologies in MoD.
3. Plans and programs for the actual realization of the information strategy of the MoD.

MoD Programming Council

The Programming Council of MoD is the main advisory organization preparing suggestions for the policy formulation, coordination and control over the execution of projects and programs related to the modernization and re-equipment of the armed forces with C4I systems (as well as other systems, armaments and equipment).

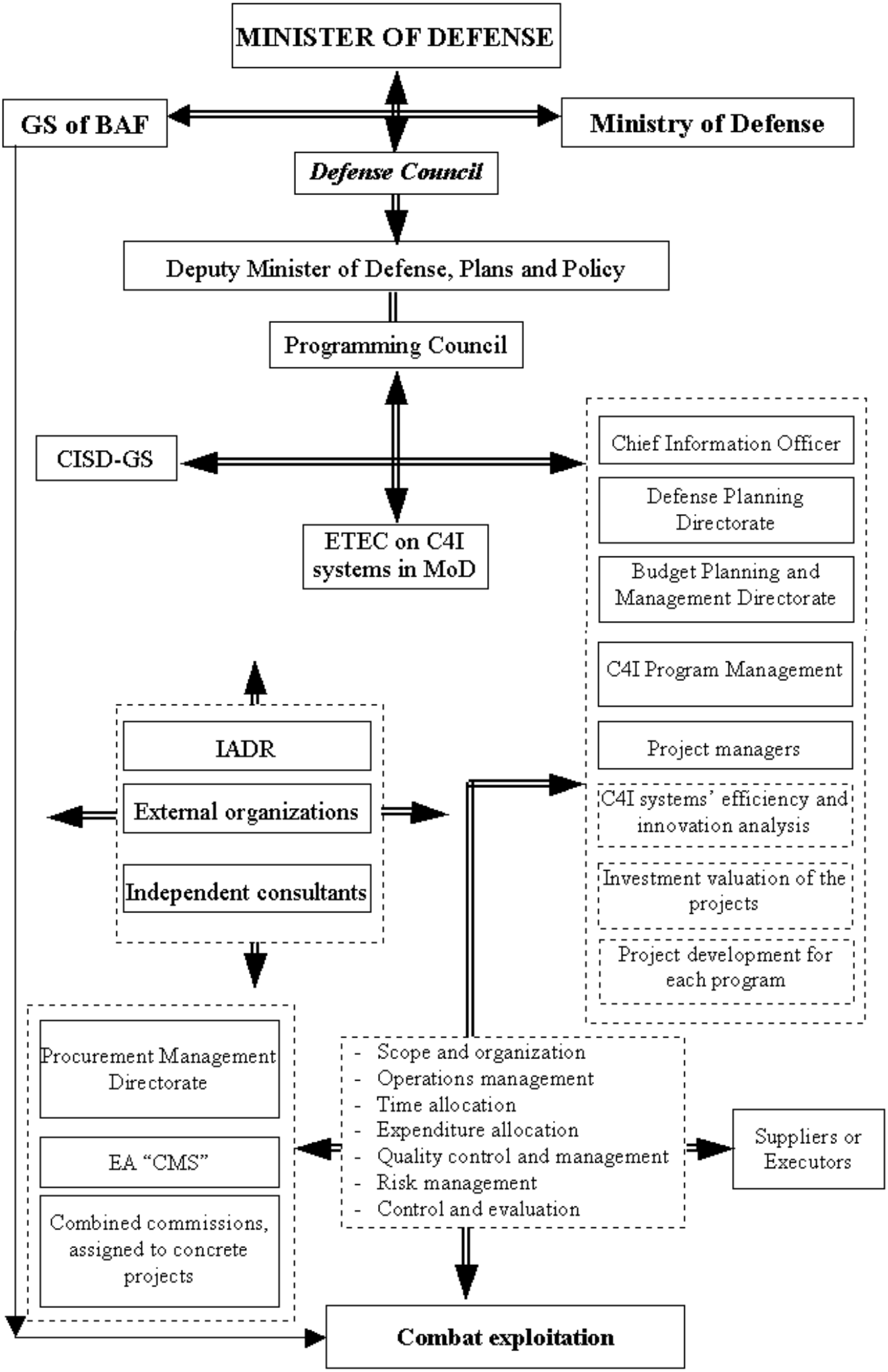
Expert Technical-Economic Council on C4I systems (ETEC on C4I)

ETEC on C4I is an advisory organization of the Programming Council on C4I systems. Taking into account the analysis of independent experts, ETEC decides on the adoption of initial requirements and concepts of developing and/or modernizing C4I systems. For those purposes, a list of approved experts is submitted and adopted annually in ETEC. The experts are renowned scientists in various fields of science and technology related to C4I systems.

Scientific-Technical Commissions on C4I systems (STC on C4I)

The STC on C4I are established in:

1. the central administration of MoD
2. services, departments and commands that use C4I systems and are directly subordinate to the General Staff.


MINISTER OF DEFENSE
GS of BAF
Ministry of Defense
Defense Council
Deputy Minister of Defense, Plans and Policy
Programming Council
CISD-GS
ETEC on C4I systems in MoD
Chief Information Officer
Defense Planning Directorate
Budget Planning and Management Directorate
C4I Program Management
Project managers
C4I systems' efficiency and innovation analysis
Investment valuation of the projects
Project development for each program
IADR
External organizations
Independent consultants
Procurement Management Directorate
EA "CMS"
Combined commissions, assigned to concrete projects
- Scope and organization
- Operations management
- Time allocation
- Expenditure allocation
- Quality control and management
- Risk management
- Control and evaluation
Suppliers or Executors
Combat exploitation

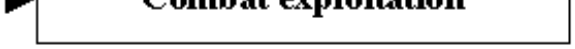


Figure 3. C4I systems life cycle management

They are additional advisory organizations, of the respective commanders and directors, that create programs and solve concrete problems in the course of the development, modernization, implementation, combat use, technical exploitation and maintenance of C4I systems. Apart from the concrete scientific-technical problems in the above-mentioned fields, the STC reviews and gives opinions about the documents on C4I systems that are submitted to ETEC.

Life cycle model of C4I systems

The life cycle model of C4I systems, as presented in "Manual for C4I Life Cycle Management in the Ministry of Defense and the Bulgarian Armed Forces" [3] is as follows:

(1) In accordance with C4I systems' requirements set by various users (MoD, GS, service headquarters, central commands), concepts, programs and initial requirements are developed and then submitted to the Defense Planning Directorate.

(2) The Defense Planning Directorate systematizes and compares the submitted proposals with the plans and programs for development of MoD and BAF and then sends them to ETEC for consideration along with its own position on the subject.

(3) On the approval by ETEC, the concepts, programs, plans and initial requirements are sent to the Defense Planning Directorate (DPD). Along with its own position, the DPD submits them for consideration in the Programming Council.

(4) The Programming Council considers the submitted proposals for new C4I systems or modernization of old ones and then confides the organization of developing Tactical-Technical Requirements (TTR), system products and prototypes to the DPD.

(5) The results from the research (planning) are put in writing as Technical-Economical Report (TER) and TTR (project) and submitted for consideration in ETEC.

(6) The approved TTRs and TERs are then submitted for consideration in the Programming Council.

(7) The Programming Council considers the submitted TTRs and TERs , sets them in order of priority and issues a position in the Defense Council.

(8) After the Defense Council has considered the TTRs and TERs the Minister of Defense approves them, orders the initiation of the programs/projects and appoints a program/project manager. The latter supervises and bears full responsibility for the program's completion.

(9) The scientific supervision in the course of the projects' experimental-design stages is done by the IADR. The Procurement Management Directorate carries out activities related to commercial contracts. The EA "CMS", the Military Standardization, Certification, and Codification Directorate (MSCCD) and the Security Service in MoD are responsible for organizing the testing, correctness of standardizing documents, certifying the producers and information control and protection in C4I systems.

(10) The implementation of C4I systems is consequently considered by the C4I Expert Commission (EC C4I), ETEC, Programming Council and Defense Council.

(11) The implementation of C4I systems is done according to current standardization documents and with the help of the IADR, Information Support Center, "Information Support" Section in MoD, and the organization initiating the implementation procedures.

(12) The exploitation of C4I systems is done by the organizations for which they are designed. Statistical data is also gathered for the systems' operation in the course of their exploitation.

(13) The organization that implemented a C4I system carries out its decommissioning. The written opinion of the ETEC and Programming Council are required for decommissioning.

The developed life cycle management model, shown on Figure 3, is adopted in the "Manual for C4I Life Cycle Management in the Ministry of Defense and the Bulgarian Armed Forces", approved by the Minister of Defense.

Conclusions

The report, issued by a Bulgarian-US study team, provides a comprehensive analysis of the current state and recommendations for the development of C4I systems. It is of great importance to the MoD of the Republic of Bulgaria, and should be considered as the major document guiding the activities related to communications and information systems in the MoD. It should also guide the future development of those systems, as well as the necessary organizational measures to ensure the compatibility of the Bulgarian systems with those of NATO and the United States in order to prepare Bulgaria for NATO membership.

The meetings held in the United States on issues related to C4I systems clearly showed the importance of cooperating with the US in this advanced technology field where the Americans are world leaders. It would be largely instrumental to establish combined Bulgarian-US teams working on the top priority projects in the MoD.

After proving its indispensability, the institution of the Chief Information Officer was established in the MoD of the Republic of Bulgaria. The Chief Information Officer is responsible for development of C4I systems in MoD, coordination and management of the undertaken projects aiming at the effective use of new information and management technologies.

It is important that more Bulgarian experts are trained in the United States in communications and information systems, communications and information program management and the "CIM" program.

The Republic of Bulgaria could benefit even more from the US experience while organizing to deal efficiently with communications and information systems in the armed forces and creating the competitive market conditions for the private businesses in the field. While developing those systems not only the common use of the programming principle is essential but also the establishment of interrelations and coordination among all programs.

References:

1. *Military Doctrine of the Republic of Bulgaria*, Approved by the XXXVIII National Assembly of the Republic of Bulgaria on April 8, 1999, (Sofia: Military Publishing House, 1999). Full text in English is available at http://www.md.government.bg.
2. *Main Recommendations for Development of C4I Systems in the Bulgarian Armed Forces* (Sofia: Ministry of Defense, 2000).
3. *Manual for C4I Life Cycle Management in the Ministry of Defense and the Bulgarian Armed Forces* (Sofia: Military Publishing House, 2000).
4. Todor D. Tagarev, "The New Military Doctrine of The Republic of Bulgaria: Contribution of Communications and Information Technologies to Achieve National Security Objectives," in *Proceedings of the C4/NCMC International Conference* (Sofia, Bulgaria: June 1999), 7-17.
5. Velizar M. Shalamanov and Todor Tagarev, "The Role of Education and Training in the Field of C4I," in *Proceedings of AFCEA-Europe Budapest Seminar* (Budapest: AFCEA-Europe, 1994), 13-17.
6. Velizar M. Shalamanov, "CJTF C4I Systems for Early Warning and Rapid Reaction," in *Proceedings of the 1997 AFCEA–Europe Brussels Symposium* (Brussels: AFCEA-Europe, 1997).
7. Vladimir Dankov, "Information technology Management for the Bulgarian Armed Forces XXI," *Information & Security. An International Journal* 1, 2 (Fall, Winter 1998), 17-32.
8. *C4I Study for Bulgaria: Final Report* (USAF ESC/MITRE, January 2000).
9. *C4I Study for the Ministry of Defense of the Republic of Bulgaria: Comprehensive Analysis and Assessment of Ongoing Projects and Legacy C4 Systems and Estimation of the Level of NATO Interoperability* (Sofia: Military Publishing House, 2000).
10. JTLS – Joint Theater Level Simulation. For description the reader may refer to Ronald J. Roland, "Applying Modeling and Simulation to Enhance National and Multi-National Cooperation," *Information & Security. An International Journal* 3 (1999), 12-24.

STOYAN BALABANOV is an officer in the Bulgarian armed forces with the rank of Colonel. He received M.Sc. degree in communications engineering from the Bulgarian Air Force Academy in Dolna Mitropolia (1980) and Ph.D. degree in Radio-communications and Electronic Warfare from the Military Scientific Research Institute in Sofia (1990). Dr. Balabanov has over sixty refereed publications in the area of radio technologies and reliability. Currently, he is Associate Professor at the Institute for Advanced Defense Research of the "G.S. Rakovsky" Defense College in Sofia, Bulgaria, and works on development and implementation of tactical military communications. E-mail: sbalabanov@md.government.bg.

KARMEN ALEKSANDROVA holds a M.Sc. degree in Telecommunications engineering from Technical University of Sofia (1979) and Ph.D. degree in Radar technologies and systems from the Military Scientific Research Institute in Sofia (1995). Currently, she is Assistant Professor at the Institute for Advanced Defense Research of Bulgarian Defense Academy "G.S. Rakovsky" and works in the areas of signal detection and digital signal processing. Dr. Alexandrova has 25 refereed publications. E-mail: alexandrova_k@yahoo.com.

BACK TO TOP

Information & Security. An International Journal
e-mail: infosec@mbox.digsys.bg

C4I System Reengineering: Essential Component of Bulgarian Armed Forces Reform

Stoyan Balabanov and Karmen Alexandrova

Keywords: C4I systems, Bulgarian Armed Forces, Communications and Information Systems, Command & Control, NATO Standards.

Abstract: The article presents main results of a comprehensive study of the command, control, communications and computer systems for the Bulgarian Ministry of Defense. It outlines current and planed C4 system capabilities of the Bulgarian armed forces. Recommendations for modernizing C4I systems to achieve requirements for NATO interoperability and standards, as well as priority projects are briefly described. Finally, the authors present roles and functions of organizational structures in the process of system development, accounting for the newly established C4I systems life cycle model.

Author: **Charles R. Myer**
Title: **C4ISR Architectural Frameworks in Coalition Environments**
Year of issuance: **2000**
Issue: **Information & Security. Volume 5, 2000**
Hard copy: **ISSN 1311-1493**

C4ISR ARCHITECTURAL FRAMEWORKS IN COALITION ENVIRONMENTS [1]

Charles R. MYER

Table Of Contents:

The break-up of the Soviet Union unleashed a flood of nationalism throughout Southeastern Europe (SEE). Freed from the yoke of suppression, the nations of the region sought economic stability and security in a dramatically changing global environment. These nations are anxious to display Western leanings and to ensure national security through multinational regional coalitions. These coalitions, in turn, are being supported by a variety of national, NATO, and U.S. sponsored initiatives with the common goal of regional stability.

The common thread through these SEE initiatives is the use of Information Technology (IT) to improve Command, Control, and Communications (C3) in a combined military/peace support domain. This paper proposes an IT-driven Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Architectural Framework approach to the integration of combat and peace support forces in regional coalition initiatives. Although the framework is applicable across the total C4ISR domain, only Command, Control, and Communications are relevant to the subject addressed in this paper and will be the term used throughout. Computers are assumed as a logical part of C3.

This paper also proposes that this type of architectural approach is applicable to other possible regional coalitions on a global basis.

The Coalition Environment

For nearly a decade following the break-up of the Soviet Union, the newly freed nations of SEE directed their

energies internally. Military reform, political instability, economic upheaval, and severe budgetary constraints and re-directions were but a few of the crises that were ultimately abated through newly adopted democratic processes. Concurrently, the stirrings of "coalition" had begun as the need for regional stability grew stronger.

The origin of SEE coalitions dates back to 1990 when NATO first extended "a hand of friendship'' to all ex-Warsaw Pact States. Within a year, NATO endorsed the establishment of the North Atlantic Cooperation Council (NACC). The NACC charter was "to commence planning with liaison countries on disaster relief and refugee programs and other security challenges in Europe." Two years later (in 1993), a U.S. Office of the Secretary of Defense (OSD) Policy Paper was approved by the NACC and endorsed by NATO. The term "Partnership for Peace (PFP)" emerged from that paper. Shortly thereafter, the U.S. Secretary of Defense—Les Aspin—publicly described the 5 "big advantages" of the PFP for both allies and partners: [2]

1) The PFP does not re-divide Europe.

2) The PFP sets up the right incentives. In the new post-Cold War world, NATO can be an alliance based on shared values of democracy and the free market. The PFP rewards those that move in that direction.

3) The PFP requires that partners make a real contribution. Security consultations with NATO, for instance, are offered only to States that are serious about playing the game.

4) The PFP keeps NATO in the center of European security concerns and, thereby, keeps American involvement at the center of Europe.

5) The PFP puts the question of NATO partnership for partners where it belongs, at the end of the process rather than at the beginning. (Another way of saying partners must first pull their own load for partnerships to solidify.)

From this beginning, the PFP has become the foundation for nearly all coalition efforts that have evolved within the SEE nations.

The Coalition Initiatives

The key PFP coalition initiatives that emerged from this origin, and on which this paper is based, are discussed below.

The PFP Information Management System (PIMS)

PIMS was initiated with U.S. funding, and it has received continued U.S. support. Also, PIMS provides a LAN-based host infrastructure and broadband satellite-based network access to each PFP nation that has elected to participate in the PIMS Program. A typical PIMS network is shown in Figure 1.

The various PIMS national hosts (e.g., Bulgaria) are linked with each other and with NATO/U.S. PIMS support Agencies via the Internet or E-mail. Connectivity is provided by 2-way VSAT or FDDI cable. PIMS support nodes are shown in Figure 1.

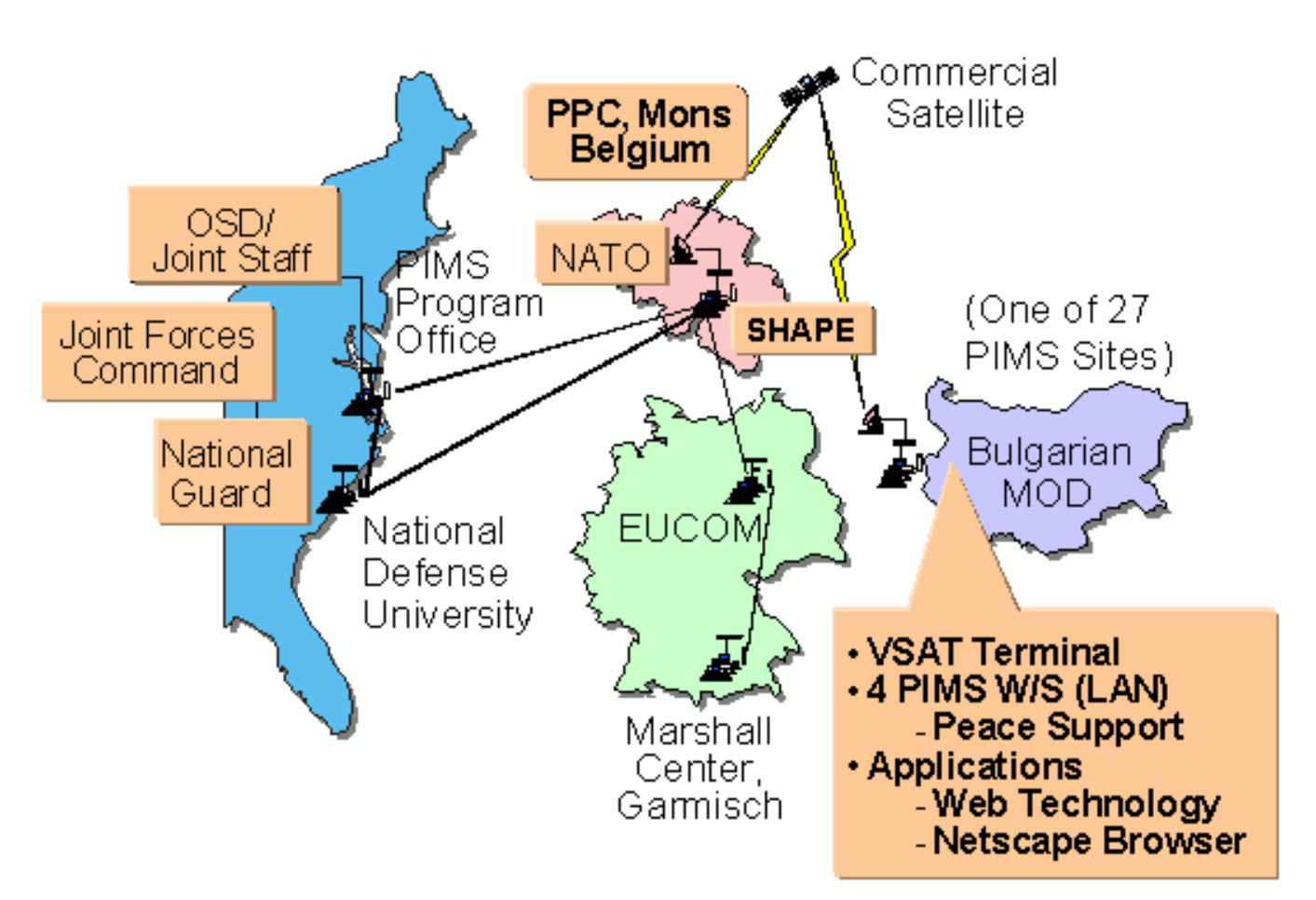


Figure 1. PIMS Hosts and Network Connectivity

As a part of the PIMS Program, each PFP host nation is partnered with a U.S. National Guard Unit located in one of the U.S. States. Each partnered Guard Unit also has a PIMS LAN. This linkage provides the coordination, exchange, and collaboration of information covering a variety of global peace support applications resident on PIMS host servers. PIMS unclassified information exchange includes collaborative operational and planning data that are relative to peace support actions.

The SEE Defense Ministerial (SEDM) Process

The Ministers of Defense of nine nations (Albania, Bulgaria, The Former Yugoslavian Republic of Macedonia (FYROM), Greece, Italy, Romania, Slovenia, Turkey, and the United States) signed an agreement to establish the SEE Defense Ministerial (SEDM) process. The SEDM engenders cooperation and dialog among the countries of SEE to foster regional security, stability, and good neighborly relations. The SEDM has generated numerous internal PFP-based regional initiatives. The more significant of these initiatives are as follows: [3]

- On September 26, 1998, seven of the SEDM nations (Bulgaria, Romania, FYROM, Italy, Albania, Turkey, and Greece) agreed to participate in the activation, manning, and support of a Multinational Peace Force South-Eastern Europe. The initial force is a Brigade. The mission of the Brigade, named the Multinational Peace Force Southeast Europe (MPFSEE), is to contribute to regional security and stability in the Euro-Atlantic area and to foster cooperation among SEE countries. Slovenia and the United States are only SEDM observer nations, but they have expressed their full support and determination to contribute. The MPFSEE has been activated in Plovdiv, Bulgaria in a new military compound provided by the Bulgarian Government. Currently, military personnel from all seven

participating nations man the MPFSEE. The MPFSEE domain is shown in Figure 2.

- In June 1999, the SEDM launched a construction engineering initiative to aid Kosovo post-conflict reconstruction. The initiative establishes an Engineer Task Force to respond to construction-oriented humanitarian and infrastructure challenges. The effort will, in the long-term, evolve into an SEE Construction Brigade (SEECONBRIG) to complement the MPFSEE cited above.
- At the same SEDM Summit, an initiative was launched to create a Crisis Information Network (CIN) by expanding the reach of PIMS. This expansion would include enhanced W/S and server capability, satellite bandwidth, crisis management functionality, or other upgrades to meet new crisis management requirements. Video Teleconferencing, C2 systems (heretofore excluded from PIMS), digital libraries, and modeling and simulation commercial-off-the-shelf (COTS) products are candidates. To date, firm requirements for the CIN have not been defined.

Figure 2. The MPFSEE Domain

The following U.S. sponsored coalition initiatives are also in the planning stage. Though currently outside the SEDM charter, they will impact SEDM goals and objectives.

An initiative undertaken by the U.S. DoD to develop a Civil/Military Emergency Planning (CMEP) capability to be offered to all PFP nations, to include those in the SEDM.

A Global Disaster Information Network (GDIN) as a means of exchanging information between CMEP sites. Currently, the security classification of the GDIN is undecided.

The Issues of IT/C2 and Common Enterprise Architectures

When addressing regional coalitions such as PFP/SEDM, Command and Control (C2) assumes a broader significance than its more traditional combat support role. Accelerating advances in IT provide the means of enhancing C2 in both the military and civil domains for peace support. IT processes, in one form or another, provide C2 Command and Operations Nodes and Centers with a common operational picture, a complete awareness of the situation, and the ability to collaboratively plan and implement the military or civil response.

Unity of effort among coalition partners, however, is not possible if the initiatives are discordant. A common architectural thread, woven through these diverse coalition efforts, offers the best means to bring accord, thus avoiding duplication of effort, fragmentation of resources, and development of diverse technical standards.

An Enterprise Architectural Approach Defined

The U.S. DoD, over the past decade, has developed costly C3 systems without an architectural foundation. The resulting C3 systems have often failed to meet user requirements, been interconnected over inadequate communications systems, and lacked proper security and interoperability in Joint Operations. As a result, the U.S. DOD has mandated that no C3 systems will be proposed by U.S. Joint Warfighting Commanders in Chiefs (Pacific, Atlantic, Europe, Southern Region, etc.) unless the proposed system is firmly based on a C4ISR Architectural Framework. This insistence on development of an Architectural Framework before funding approval is slowly gaining global acceptance. This paper proposes this C4ISR Architectural Framework as the best way to integrate SEDM/PFP regional coalition C3 initiatives. The foundation of the Framework is shown in Figure3.

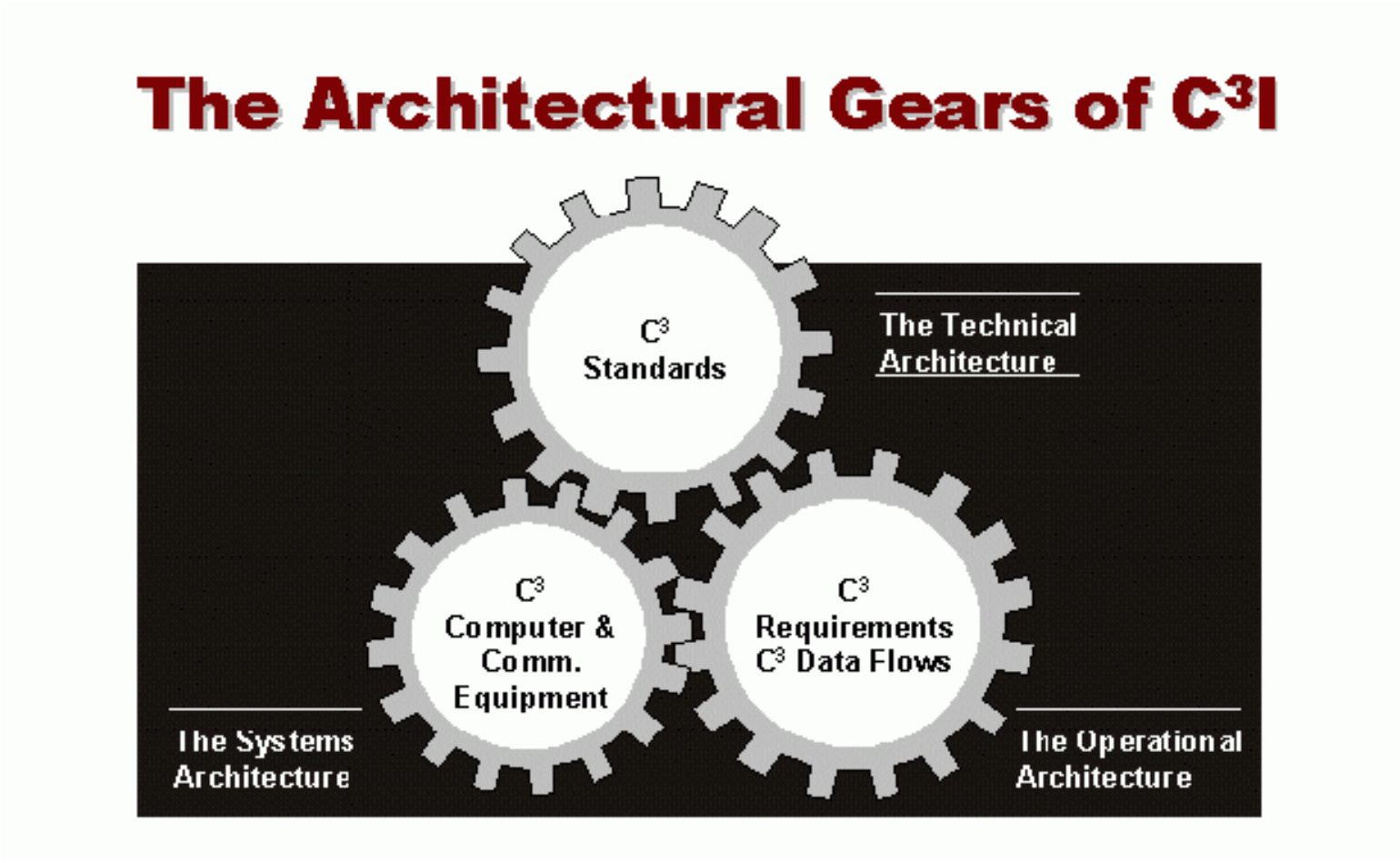


Figure 3. The C4ISR Architectural Framework

The Framework, like a gear train, develops 3 distinct—but coupled—architectures:

1. A Technical Architecture (TA) that defines current and emerging C4ISR standards for both requirements development and systems design. The standards are analogous to a blueprint for a house.
2. An Operational Architecture (OA) that defines C4ISR requirements, the resulting data flows between command nodes and the network connectivity needed to transmit and receive the defined data flows. The Operational Architecture is analogous to building blocks for a house.
3. A Systems Architecture (SA) that defines the technical parameters of hardware and software components needed to satisfy the OA. The SA is analogous to furnishing a house.

An Enterprise Architecture Approach Applied

The Environment

How do we apply this architectural methodology to the myriad of PFP-driven coalition initiatives now emerging in SEE? We can look at the challenge as a 3-circle Vinn diagram.

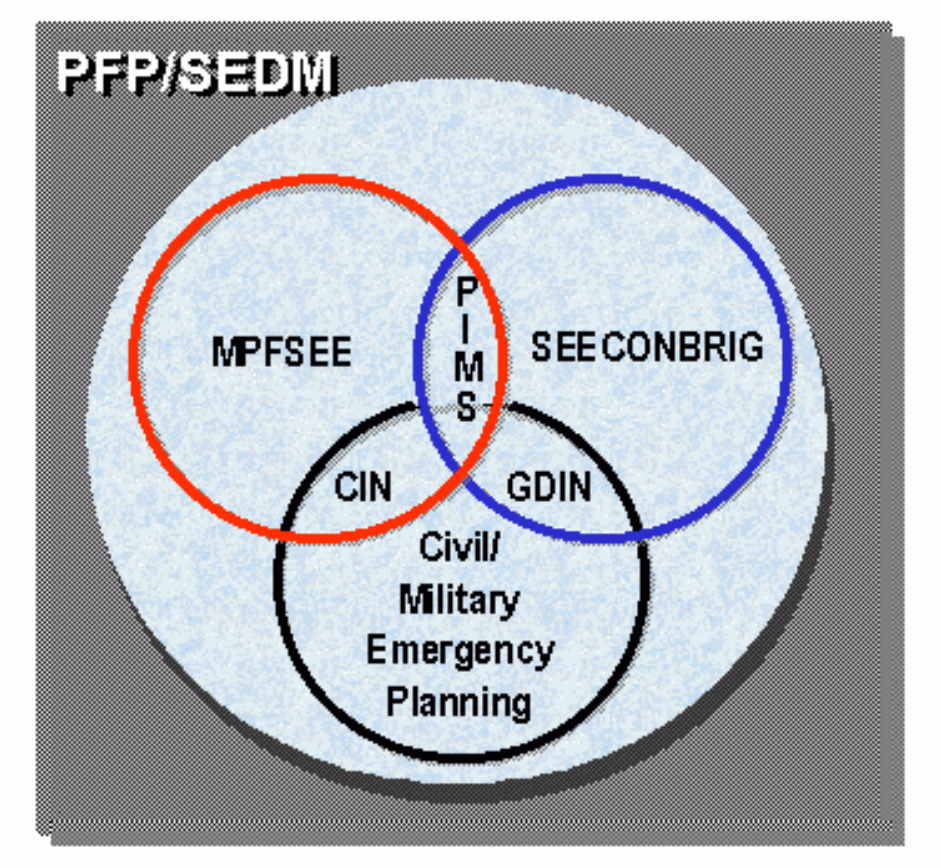


Figure 4. The SEE Coalition Initiative Challenge

Within the Architectural Framework domain, the architectural solution must encompass the six cited SEE coalition initiatives generated by PFP/SEDM-sponsored actions. This includes the following:

- Three C2 organizations or systems (MPFSEE, SEECONBRIG, CMEP). Each will generate C2 data

for transport by any of the three network initiatives.

- Three communications initiatives (PIMS/VSAT, CIN, and GDIN). Each will be networked to meet the C2 requirements of the three C2 organizations or systems.

The task is to apply the three architectures of the Framework to define the coalition C3 requirements and hardware/software characteristics that will meet the goals and objectives of the PFP/SEDM domain, as described above. Each of the three architectures is addressed in relation to that task.

The Technical Architecture

Setting common technical standards through the Technical Architecture is of crucial importance given the number of countries involved in the PFP/SEDM initiatives, all with different legacy C3 systems. These standards, applied to the operational and systems architectures, ensure the development of compatible C3 systems interoperable with NATO C3 systems. The initial list of standards selected will, however, be dynamic—changing through additions or deletions as the architectural process progresses. [4]

The Operational Architecture

Developing the OA for the mix of six initiatives, all with multinational interests, seems a daunting task but one that must be accomplished if six diverse C3 development efforts are to achieve commonality both between the efforts and the integration of these systems with NATO. The key OA products proposed are shown in Figure 5.

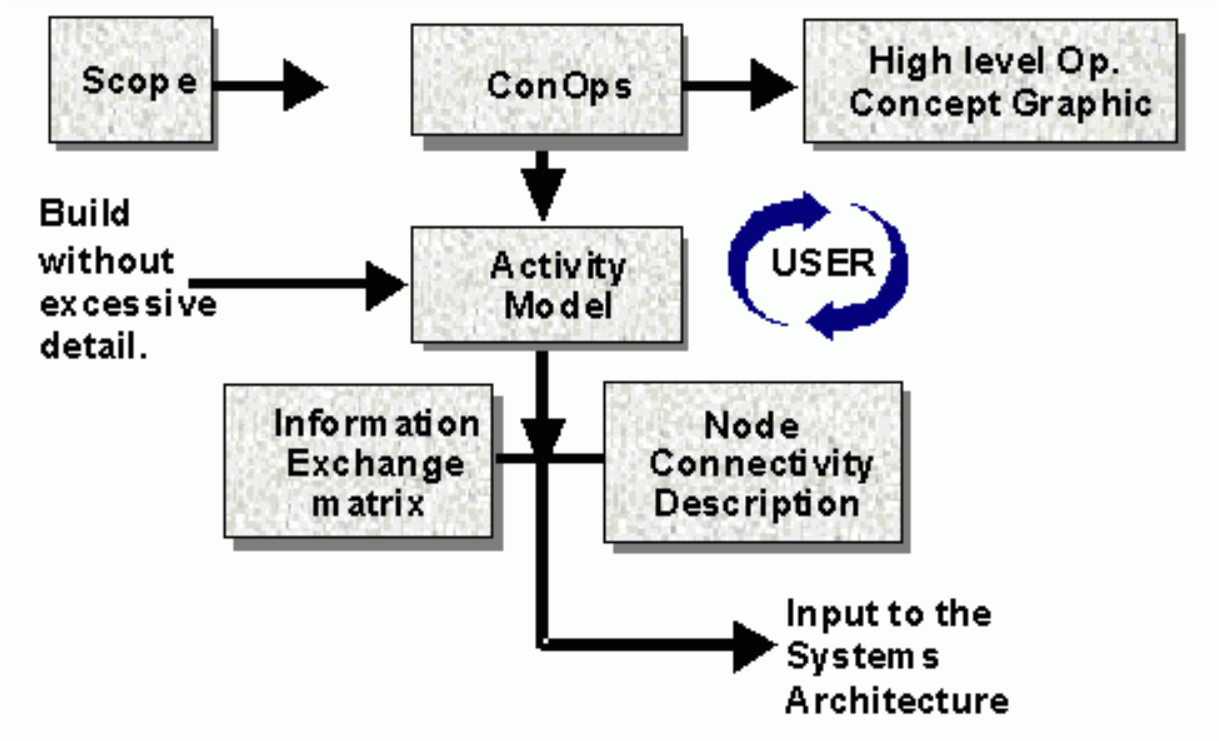


Figure 5. The Operational Architecture - Key Products

Scope

A key to successful Framework development is to limit the scope of the OA to the minimum consistent with providing adequate products to the SA. Neglecting this simple step has spelled doom for many C4ISR

Framework efforts. Defining requirements, data flows, and connectivity to a cumbersome level can result in voluminous, near-useless product inputs to the SA.

Concept of Operations (CONOPS)

The true driver of the Operational Architecture is the CONOPS. The CONOPS must be succinct and objective. As a baseline, it should use the 6 crucial factors that U.S. Joint Forces apply in defining user interest in all system development efforts. These 6 factors are briefly addressed below:

1. Doctrine: How will the user employ his or her military/crisis forces to perform his or her coalition mission?
2. Training: How will the user train his or her people to employ the doctrine?
3. Leadership: What principles of leadership development will the user follow to ensure mission accomplishment within the coalition environment?
4. Organizations: What organizational concepts will the user follow to support both national goals and coalition missions?
5. Materiel: What materiel characteristics (human factors, user unique modes of employment, etc.) apply to fit both national and coalition tasks?
6. Soldier: The key factor! What added features apply to make the soldier feel comfortable working in both his or her national and coalition environments?

The Activity Model

The most difficult product of the OA. The Activity Model must, in as little detail as possible, decompose the common coalition C2 functions to the minimum number of tasks considered necessary for NATO/SEDM/PFP Joint Crisis Action. The functions and tasks, once approved, become the functional baseline for the OA. The 3-dimensional matrix on figure 6 portrays a small slice through the Activity Model process.

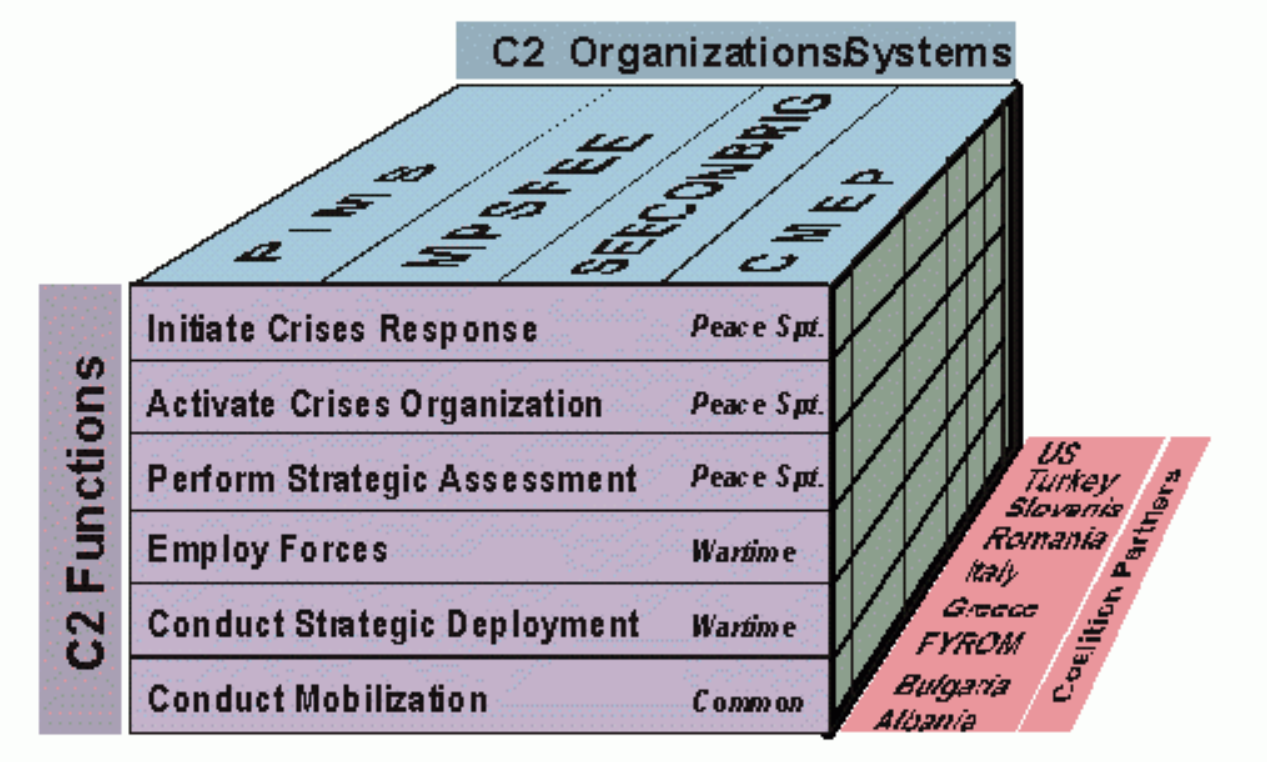


Figure 6. The SEDM Requirements Decomposition Process

Six sample functions are shown in the slice: three Peace Support functions, two Wartime functions, and one function that is common to both Peace Support and Wartime. The success of the activity Model depends on horizontal coordination between the three 3 SEDM C2 entities and the vertical coordination between each C2 function/task entity and the 9 SEDM partners in defining each function and the associated tasks.

Then, the resulting task list determines the information flows between C2 Nodes and the Connectivity Descriptions for the information flows to complete the OA. Examples are shown in Figure 7.

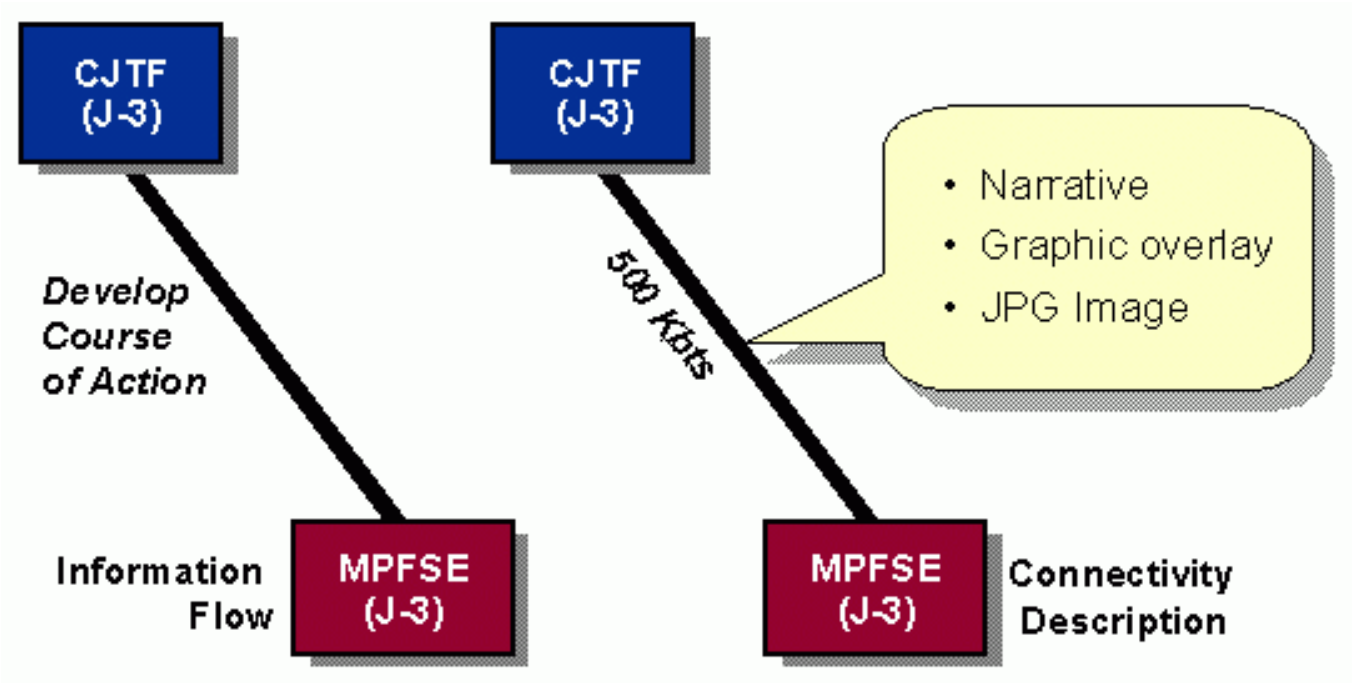


Figure 7. Examples of Information Flow and Connectivity Descriptions

The Systems Architecture

In a normal C4ISR Framework development, the SA defines hardware/software parameters for a civil or military C4ISR system. An example is the U.S. Army development of a fully digitized Corps. Operational and Systems Architectures have either been—or are being—developed for both the Corps and the major sub-elements of the Corps.

In applying the Architectural Framework in a coalition environment, the objective is quite different. The objective is not to define new C3 systems to replace national, civil, or combat force legacy systems in each country of the coalition. The objective is to determine a common and agreed-upon set of equipment characteristics and interfaces for both C2 and communications systems that are acceptable to the total coalition.

The coalition has the responsibility of obtaining the necessary hardware/software components to meet the SA parameters. Each coalition partner, having approved the OA, must, then, through their own means, provide legacy systems that are compatible with the SA design, or they must acquire new hardware/software components that are compatible. The essential products of the Systems Architecture that are consistent with this objective are shown in Figure 8.

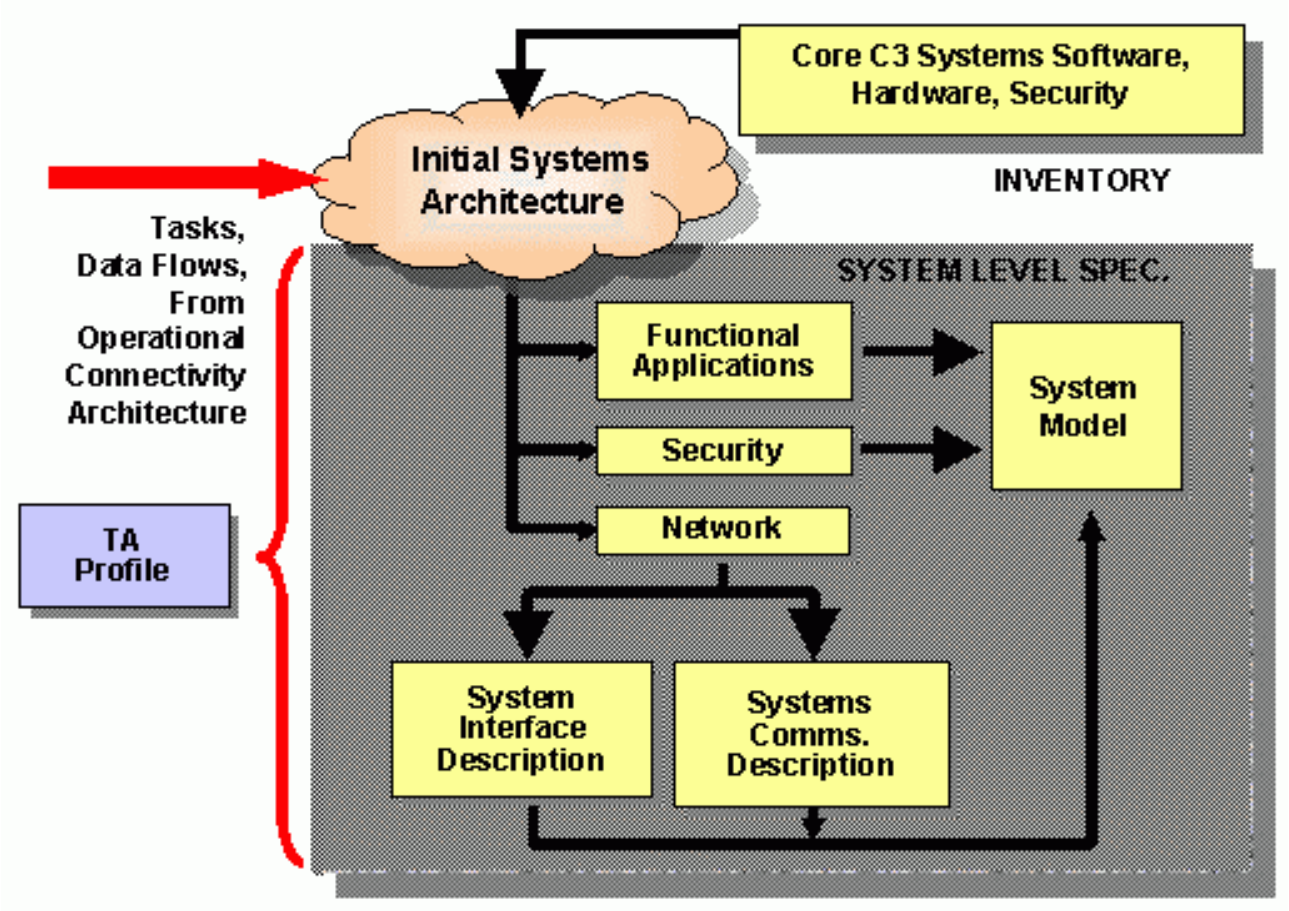


Figure 8. The System Architecture Products

The first product of the SA is an initial C3 Systems Architecture. The OA has defined the information exchanges and connectivity requirements. Based on these OA products, the Core Systems inventory for each coalition partner catalogs national legacy C2 system candidates, irrespective of operating standards, that may meet some of the OA requirements. These national systems set the initial C2 baseline. In like fashion, legacy Wide Area Network (WAN) communications systems, both national and international, are catalogued to set

the communications network baseline. Together, the C2 and communications systems define the initial C3 architecture. The initial architecture ensures optimum use of all national legacy inventories that may be compatible solutions to the final SA design parameters. The initial architecture also identifies functional, network, and security shortfalls that will drive the development of the subsequent SA products.

The shortfalls of the initial C3 architecture in standards compliance, information exchange, security, and connectivity define the tasks that the remainder of the SA development must address. Standards shortfalls are key because standards drive all other SA tasking. The standards shortfalls aid in determining standards entries in the initial version of the SA Technical Architecture Profile. The SA Technical Profile is a dynamic product to which other standards will be added or deleted as the SA proceeds. In addition, the Profile guides the subsequent development of the functional, network, and security sub-architectures as the shortfall tasks derived from the initial architecture are addressed and resolved.

It is beyond the scope of this paper to address the cumulative tasks involved in completing the functional, security and network descriptions of the SA. As a simple example, functional application needs, as defined from the OA and initial architecture shortfalls, may require trade-off analyses of competitive COTS products to determine cost-effective OA compliance characteristics.

As a final step, the applicable C3 systems candidates from the initial architecture, the detailed description of the required functional applications, the security architecture, and the coalition network design parameters are combined in a systems-level specification that will govern national or coalition-wide acquisitions.

Pulling It All Together

Developing an overall C3 architecture for a multinational coalition poses a distinct challenge. Conversely, a failure to accept the challenge invariably leads to C3 products that fall woefully short of objective performance. It is the author's opinion that a Framework, as defined above, offers the best architectural approach to the defined task. The Framework, although portrayed within a SEE regional coalition domain, is equally applicable on a global basis.

References:

1. An earlier version of this paper was presented at the AFCEA Europe 21st Symposium and Exposition "TechNet Europe 2000," Prague, Czech Republic, 18-20 October, 2000.
2. Gerald B. Solomon, *The NATO Enlargement Debate, 1990-1997. The Blessings of Liberty,* The Washington Papers 174 (Westport, Conn.: Praeger, 1998).
3. South East Europe Crisis Information Website, *Assistant Secretary of Defense Frank Kramer Proposal,* http://server.pims.org/Desktop/Topics/CivilEmerg/sedm/Kramer brief ht.
4. *NATO Open Systems Environment, Base Standards*, Version 3.1, 5 December 1997. Available at http://www.nc3a.nato.int/ppdiv/nose/nosevol4.htm.

LTG (Ret.) CHARLES MYER served in the US Army from 1943 to 1981, retiring after 37 years' active duty. He spent 12 years in command positions, company through brigade, including Vietnam commands in 1965 and 1971. His last assignment was as deputy director general, NATO Integrated Communications Systems Management Agency. Other major assignments included Army assistant chief of staff for communications and automation, and commander, U.S. Army Signal Center and

School, Fort Gordon, Ga. Currently, he is senior military adviser in Unisys Corporation and has also served at Unisys as director of business strategies, responsible for Army and joint C3I tactical/strategic planning and developing acquisition/proposal opportunities; he focused on expanding service, joint and Defense Information Systems Agency involvement in multiservice contracts related to command, control, communications, computers, intelligence, surveillance and reconnaissance. Previously, for 10 years he was with Atlantic Research Corporation as senior defense adviser, responsible for developing systems engineering and integrating acquisition and proposal planning across the spectrum of C4I disciplines. Later he was vice president and general manager of the C4I Division, responsible for initially developing the tactical network-management systems and Tactical Army Automated Computer System, the Army's first tactical computer.

General Myer authored "*Division-Level Communications 1962-1973,*" part of the Vietnam Studies Series published by the Army in 1982. His civil awards include first recipient, Fubini Award; National Security Industrial Association Person of the Year for 1994; and chairman of the NSIA study on "Army C4 modernization" sponsored by the Signal Center. LTG Myer's military awards include the Legion of Merit with two oak-leaf clusters and the Meritorious Service Medal. The Signal Regiment inducted him as a Distinguished Member in 1997. Address: Unisys Corporation, 8008 Westpark Drive, McLean, Virginia 22102. E-mail: cbobmyer@aol.com.

BACK TO TOP

C4ISR Architectural Frameworks in Coalition Environments

Charles R. Myer

Key words: C4ISR systems; operational, technical, system architectural frameworks; coalition C2, PIMS, MPFSEE.

Abstract: Nations in Central and Eastern Europe seek economic stability and security in a dramatically changing global environment. These nations are anxious to display Western leanings and to ensure national security through multinational coalitions. These coalitions, in turn, are being supported by a variety of national, NATO, and U.S. sponsored initiatives with the common goal of regional stability. The common thread through these initiatives is the use of Information Technology to improve Command, Control, and Communications (C3) in a combined military/peace support domain. This paper proposes an IT-driven Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Architectural Framework approach to the integration of combat and peace support forces in regional coalition initiatives. Although the framework is applicable across the total C4ISR domain, only Command, Control, and Communications are relevant to the subject addressed in this paper. This type of architectural approach is applicable to other possible regional coalitions on a global basis.

Author: **Vladimir Grigorov**
Title: **Engagement of the Ministry of Defense and Bulgarian Armed Forces in Establishing Information Society**
Year of issuance: **2000**
Issue: **Information & Security. Volume 5, 2000**
Hard copy: **ISSN 1311-1493**

ENGAGEMENT OF THE MINISTRY OF DEFENSE AND BULGARIAN ARMED FORCES IN ESTABLISHING INFORMATION SOCIETY

Vladimir GRIGOROV

Table Of Contents:

Introduction

The transition to Information Society (IS) has no alternative. The question of national concern, that we face now, is not whether IS should be established, but rather what are the best ways to do it. The transition to IS is an international, transcontinental process, in which separate countries carry out their national policies.

With the Decree # 679 of 29 October 1999 the Council of Ministers adopted a *Strategy for Development of Information Society in the Republic of Bulgaria* [1] and a *National Program for the Development of Information Society*. [2] With this Decree the Bulgarian Government clearly showed its understanding of the importance of IS in almost all spheres of our administrative and political life.

The new strategic vision of the MoD authorities, as part of the Bulgarian Government, is oriented towards utilizing military formations in an international environment, participation in operations other than war and their application to prevent any potential threat to the national security. The significance of the technological innovation and the challenges of establishing IS receive adequate treatment in a number of both academic studies [3] and main security and defense policy documents.[4,5] The awareness that information dominance is a prerequisite for realizing new operational concepts and achieving synergetic effect from the integral utilization of military power in all types of military operations is becoming more profound.[3,5]

In the past few years, the issue of the Information Society (IS) established itself worldwide as one of the main topics on high-level political forums. The Information Society development poses before governments a number of complex issues related to various fields of public life and requiring coordinated action. In Bulgaria, by Decree # 40 of 1998, the Council of Ministers established *Coordination Council on Information Society Issues*. Its basic function is "to develop and submit for approval by the Council of Ministers the strategy and the national program for the Information Society development in the Republic of Bulgaria."

Strategy and National Program for Development of IS

The challenge of preparing a strategy for the Information Society stems from the short time and its great scope - the IS issues concern all sectors of public and economic life. At the same time, the activities for the transition to Information Society are seen as vitally important for the Bulgarian integration into the European Union. The Strategy for Information Society development in the Republic of Bulgaria defines national priorities for transition to IS at legislative, technological, economic and social levels and outlines main related activities. The document combines the IS concept of the European Union with the national interests and the specific realities of our country, thus focusing on:

- consolidation of the democratic system;
- preparation for European and Euro-Atlantic integration;
- market economy development;
- functioning of the Currency board.

The document is developed in conformity with the Governmental Program "Bulgaria 2001" and takes into account related documents of ministries and other state agencies. Representatives of the Bulgarian Institute of Legal Development, Bulgarian Academy of Sciences, Bulgarian Telecommunications Company, National Chamber of Business Development, and the Information Society Development Association were involved in its preparation. The document takes into account the European Union strategy, national strategies and programs for transition to IS of developed countries and related documents of a number of European countries. Political and legal documents of the European Union, the Council of Europe and other international organizations were thoroughly studied, too.

Based on the Strategy, National Program for the Information Society development in the country was developed. State organizations are also preparing strategies and programs, outlining goals and intentions for the transition to the Information Society related to the sector they cover. The document "Strategy of the Information Society Development in the Republic of Bulgaria" is periodically updated and amended in accordance with developments at international and national level.

The Information Society appears as result of the changes caused by the massive introduction of new information and communications technologies (ICT). As stated in Decree # 40 of the Council of Ministers, "the Information Society is a society with qualitatively new structure, organization and

public relations, based on global access and usage of information and communications networks and services free of national, geographic or any other restrictions, for exchange of information, scientific, intellectual, cultural and other achievements." Accordingly, basic characteristics of IS are:

- utilization of information and communications technologies in all economic and social activities;
- de-massification of social and economical processes [6] - small-series production, market segmentation, disintegration of some of the big industrial companies, etc.;
- high employment in the area of services - over 50 percent of the whole working population;
- continuous process of qualification in dynamically changing environment requiring lifelong learning and self-education;
- enhancement of the social role of the individual - the changes in the nature of labor and management enhance the individual’s responsibility;
- globalization, economic and social cohesion - conditions are created for building a "society without frontiers," for elimination of "distances," for transition towards social uniformity.

The transition to IS has no alternative. A matter of national choice is not whether IS will be built, but what are the best methods and forms for its realization. The transition to IS is a trans-border and transnational process in which the states pursue their particular national policies.

In recent years, the technologically developed countries like the United States, EU member-states, etc., adopted strategies and programs for transition to the Information Society. Such documents are prepared by almost all countries of Central and Eastern Europe (Romania, Estonia, Hungary, Slovenia, Latvia, Lithuania, etc.). These acts outline the integrated framework for IS and encompass key sectors, such as telecommunications, scientific research and development, innovations, competitiveness, small and medium enterprises, economic and social cohesion, intellectual property, data protection, electronic commerce, international relations and cultural exchange.

Globally, the following core principles of the policy for IS development are set forth:

- promoting competition;
- encouraging private investments;
- defining an adaptable regulatory framework;
- providing open access to networks;
- ensuring universal information services;
- promoting equal rights of access to information resources;
- promoting diversity of content, including preservation of cultural and linguistic diversity;
- recognizing the necessity of worldwide cooperation with particular attention to less developed

countries.

While establishing the IS, Bulgaria has to find an adequate national expression of these principles.

In view of the global trends of the Information Society development and the Bulgarian conditions, the basic goals that have to be achieved in the process of transition to IS in Bulgaria are:

- preparation and adoption of a complete legal framework, rules and procedures, harmonized with those of the European Union, for provision of services, for living and working in the Information Society;
- ensuring equal access for all citizens to modern, efficient and high-quality telecommunications and information services, as well as equal opportunities for acquiring skills for their utilization;
- creation of new living and working environment through wide use of new ICT in the public, political, economic and cultural sphere.

In order to achieve the goals for transition to IS, the following action should be undertaken:

- introduction of European norms of ensuring access to information while guaranteeing data security and basic human rights;
- creation of a transparent and predictable legal and regulatory framework for provision of Information Society services to the population and businesses;
- getting the national standardization system in conformity with the international requirements;
- development and modernization of the telecommunications infrastructure as a basis for building the national information infrastructure;
- provision of telecommunications, media, multimedia and information services in a liberalized environment, with clear mechanisms for respecting the rights of citizens and consumers;
- introduction of modern ICT in management, economy, education, culture, health care, national security, ecology;
- updating the functions, structure, products and services of administration and business in accordance with the new ICT and creation of conditions for sustainable development;
- development of information, communication and audiovisual/multimedia industry based on the principle of non-discrimination and fair competition;
- ensuring conditions for common education, continuous and individualized ICT training;
- training highly qualified ICT specialists;
- establishment of the necessary conditions for complete use of the opportunities for employment in IS;
- utilization of the new ICT for preservation of national traditions, culture and identity;

- wide awareness and preparation of the society for complete realization within IS.

Contribution of the Ministry of Defense

The responsibility for realizing this strategy lies with the Coordination Council on Information Society Issues. This specialized body to the Council of Ministers takes decisions at national level. It monitors and coordinates the mutual interests, needs and activities of the state bodies aimed at realization of the goals and tasks included in the Strategy and in the National Program.

The Ministry of Defense is represented at the Coordination Council on Information Society Issues by the Deputy Minister on Defense Policy and Planning and the Deputy Chief of General Staff (GS) on operations. The Deputy CIO (Chief Information Officer) assists the permanent working group of the Coordination Council. IT specialists from the MoD and armed forces participate in various work groups that assist the Coordination Council.

As a result of the effort of the MoD representatives in the Coordination Council the following points were added to the list of recommendations for the operation of the Council in 2001:

- Institutionalization of the position of "Chief Information Officer" in structures of the state administration.
- Development of regulations for implementation of information and communications systems of the state administration.
- Development of information assurance concept for the needs of the defense and security.

The Coordination Council is assisted by the Committee of Posts and Telecommunications (CPT) that conducts operational coordination with ministries and state bodies, with representatives of public organizations and institutions and with the private sector. As a state body in charge of the administration and technical support of the Coordination Council, CPT monitors, analyses and disseminates information regarding the current state and trends at international and national level with respect to IS development, organizes and coordinates national events and the participation in international forums on issues of IS.

In the particular sectors, the authorized state bodies manage and monitor the implementation of the goals and tasks, stemming from the Strategy and the National Program for IS development. They periodically inform the Coordination Council on the development in the sector, problems and need of assistance.

The new ICT also offer opportunities for more efficient communications and exchange with the European institutions in the process of Bulgaria’s preparation for joining the EU. For these reasons, specialized databases will be created, reflecting the institutions’ activities on the country’s preparation for membership. Furthermore, efficient telematic links with relevant institutions of the EU will be built.

As a whole, the development of the IS is expected to contribute to the harmonization of the relations

between administration, population and business and to strengthening of the democratic public control over the management of the country.

Defense management and strengthening the national security play a key role in the establishment of the IS in the country. It is necessary to apply consistently the principles of transparency of management and civil control of the military, on one hand, and guaranteeing the necessary degree of secrecy, on the other.

Bulgaria’s integration in NATO demands modern and efficient armed forces, adequately equipped with information and communications systems. Priority tasks in this respect are:

- Modernization of the system for command, control, communications, information and surveillance systems in the Ministry of Defense through:
    - building a system for command, control, communications, information and surveillance systems in the Ministry of Defense totally compatible both internally, and with the national communication-information systems, as well as with NATO partners;
    - implementation of advanced communications and information technologies, meeting NATO standards, in order to provide information superiority, as set forth in the Bulgarian military doctrine;
    - consistent application of the program approach and the team principle in building the systems for command, control, communications, information and surveillance systems in the Ministry of Defense;
    - ensuring reliable protection mechanisms for accessing and using information in the military communications-information systems.
- Modernization of military education and defense research through:
    - extension of the scope and updating of the educational programs in the field of ICT, in order to ensure adequate training of the command staff of the Bulgarian armed forces;
    - introduction of modern multimedia products and virtual simulators for training the staff of the Bulgarian armed forces;
    - introduction of ICT in the research and development activity in order to raise their efficiency and quality;
    - introduction of a new system for scientific and applied studies through assignment of tasks, joint development, etc.

The development and modernization of communication and information systems (CIS), as an essential element of the management information system of MoD and Bulgarian Armed Forces (BAF), is vitally important for the completion of the tasks outlined in the reform plan, known as "Plan 2004", and the Membership Action Plan. The 1999 survey of C4 systems of the BA defined the major recommendations for the development of CIS, supporting the creation of realistic plans for procurement of a fully compliant functionality, reliability and operational compatibility. The amount

of work, short deadlines and limited budget resources required the creation of an organizational structure with clearly outlined competence, responsibilities and management methods. For this purpose, a normative foundation was laid, containing the following documents:

1. C4 study recommendations [7];
2. Manual for C4I Life Cycle Management in the Ministry of Defense and the Bulgarian Armed Forces [8];
3. Concept for Planning, Programming and Budgeting and Manual for programming in the Ministry of Defense.[9]

The Manual for C4I Life Cycle Management defines conditions, rules and responsibilities of the bodies and authorities in the MoD and BAF that relate to ordering, planning, research and development activities, procurement, financing, exploitation and decommissioning of command and control systems, communications and information and intelligence systems (C4I). The Manual applies to all subsystems and software products, providing management and oversight of the basic C4I systems of MoD and BAF in both peace and crisis.

The next step, carried out in this direction, was the establishment of the institution "Chief Information Officer" (CIO) within MoD and BAF. Our decision was driven by the need to provide expert coordination and management of C4I systems projects from the start of the project to the beginning of system exploitation. The inauguration of CIO is not just an act of delegating responsibilities to the management of information technologies, but rather demonstrates the desire of MoD authorities to face the latest challenges. For example, in the United States training employees for this institution is considered a very important strategic goal. For the purposes of the US Department of Defense there is a college where future experts are educated in the field of information resource management.

The Manual for C4I Life Cycle Management and the CIO institution were introduced in MoD and BAF in June 2000 with an order of the Minister of Defense. The MoD successfully dealt with issues concerning C4I systems as well as with defense planning and programming. We are fully aware that a basic prerequisite for the success in this field are the clearly defined interrelations between:

- resources and results,
- participants and deadlines,
- constant monitoring, control and transparency of all expenses.

The development of C4I systems is realized through programs, subprograms and program modules (referred to herein as "programs") classified according to their type and level and incorporated in the "Program Decision Memorandum" of Ministry of Defense. The programs contain integrated R&D, technological, technical, organizational and economic activities that contribute to the achievement of goals related to national security and development of modern C4I systems for the MoD and BAF. Subprograms and program modules are the separate parts of a program, financed within the main program.

The programs can be classified in three level groups, according to their significance for the defense of the Republic of Bulgaria, as follows: national level, departmental level and type of armed forces level.

The programs on the national level are designed to satisfy the needs of the Republic of Bulgaria in terms of the general requirements of MoD and BAF and other departmental and state organizations such as Ministry of Interior, Ministry of Transportation and Communications, etc. Their realization requires considerable financial resources and has direct impact on the national security. The programs on the departmental level are designed to satisfy MoD and BAF requirements for modern C4I systems and relevant technical and training facilities. Their realization influences directly the readiness of BAF to perform military operations. Currently, the programs on service level are designed to solve specific problems in the field of preservation, technical exploitation and maintenance of C4I systems in the respective formations.

Another essential point in our future activities is the decision to form integrated project groups consisting of experts from all departments, involved in their respective projects. The latter has already been planned for the following priority projects [10]: Pilot Project for construction of communicational-information system in Sofia Garrison, the project for National Military Command Center, Air Sovereignty Operational Center (ASOC), the Field Communications and Information System (FICIS) for PSO designated units, teleconferencing project (DAMA SATCOM) and secure data interchange between the capitals of NATO member countries. The realization of these projects will give the necessary technological and organizational impetus to the modernization of C4I systems, thus turning them into the backbone of a future expanded system.

In compliance with Plan 2004, for the purposes of consolidating the scientific research and development activities, an Institute for Advanced Defense Research (IADR) was established in the "G.S. Rakovski" Defense College. IADR performs scientific research in the field of national security, defense and military forces. The three main areas of research are in defense resource management, C4I systems, and armaments. The IT research and development activities of the IADR are focused in the following areas:

- Advanced communications technologies;
- Information security;
- Geographical information systems;
- Modeling and simulation;
- Multimedia applications;
- Information support for defense resource management.

IADR performs its activities in close cooperation with partner scientific and research institutes, as well as with other national and foreign institutes through [11]:

- Participation in joint working groups engaged in scientific programs, projects, studies, etc;

- Exchange of experts;
- Participation in conferences, symposia, seminars, etc., related to IADR field of activities;
- Education and training;
- Specialized training and certification of IT specialists and users.

Memorandum for cooperative activities has been signed with the Bulgarian Academy of Science. Several research projects are performed jointly with high-tech business companies:

- with Cisco Systems Bulgaria – the establishment of Cisco Academy in the "G.S. Rakovski" Defense College;
- with S&T and "Baltimore" – development of a pilot model, PKI (Public Key Infrastructure) and joint research activities in the field of information security;
- with Computer Associates Plc.-Bulgaria – testing network management solutions;
- with InfoGuard Ltd. - Bulgaria – testing wireless communications systems, anti-virus protection and maintenance of workflow management systems;
- with "GIS Invest" – research and testing applications for geographical information systems;
- With IDG-Bulgaria – testing and evaluating new technological solutions.

The Bulgarian defense establishment is an active contributor to national efforts towards development of the information society. We believe that by introducing modern normative base and institutions, the Bulgarian Ministry of Defense and General Staff will be able to respond adequately to the challenges of the Information Society. In certain cases, the Ministry of Defense may serve as "national testbed" for new organizational schemes and management practices in the area of IT development, thus leading technological and cultural advancement.

References:

1. *Strategy for Development of Information Society in the Republic of Bulgaria* (Sofia: Impulse Information Publishing Center, Ministry of Transportation and Communications, 1999). Available in English at http://www.cpt.bg/en/cpt/default.htm.
2. *National Program for Development of Information Society* (Sofia: Impulse Information Publishing Center, Ministry of Transportation and Communications, 1999). Available in English at http://www.cpt.bg/en/cpt/default.htm.
3. See for example Velizar Shalamanov and Todor Tagarev, *Information Aspects of Security* (Sofia: Procon, 1996).
4. National Security Concept of the Republic of Bulgaria, *State Newspaper*, # 46, 22 April 1998 (available full text in English at http://www.md.government.bg).
5. *Military Doctrine of the Republic of Bulgaria*, Approved by the XXXVIII National Assembly of the Republic of Bulgaria on April 8, 1999 (available full text in English at http://www.md.government.bg).

6. See for example, Alvin Toffler and Heidi Toffler, *War and Anti-war: Survival at the Dawn of the 21st century* (Boston: Little, Brown and Co., 1993), 72.
7. See *Command, Control, Communications and Computers Study for Bulgaria* (Hanscom AFB, MA: Electronic Systems Center/MITRE, 2000); Main Recommendations for Development of C4I Systems in the Bulgarian Armed Forces (Sofia: Ministry of Defense, 2000).
8. *Manual for C4I Life Cycle Management in the Ministry of Defense and the Bulgarian Armed Forces* (Sofia: Military Publishing House, 2000).
9. *Concept for Planning, Programming and Budgeting in the Ministry of Defense and the Armed Forces; Manual for Developing Programs in the Ministry of Defense and the Armed Forces* (Sofia: Military Publishing House, 2000).
10. To be described in detail in the next volume of this journal.
11. "Research and Demonstration Center of the Institute for Advanced Defense Research," *Information & Security. An International Journal* 4 (2000), 143.

VLADIMIR GRIGOROV is Chief of "Programs for Development of Armaments, Equipment, and Infrastructure" section of the Defense Planning Directorate in the Bulgarian Ministry of Defense. He was born on 22 of June 1955 in Sungurlare, Bulgaria. Mr. Grigorov holds a Bachelor Degree in Information Technologies from the Military Artillery and Air Defense School, Shumen, Bulgaria, and M.Sc. Degree in Management and Development of Information Systems from the National Defense College. Until 1999, Mr. Grigorov worked in the General Staff of the Bulgarian Armed Forces in the area of Communication and Information systems management. Since 2000, he is Deputy Chief Information Officer of the Bulgarian Ministry of Defense and a member of the permanent working group to the Coordination Council on Information Society Issues.

BACK TO TOP

Engagement of the Ministry of Defense and Bulgarian Armed Forces in Establishing Information Society

Vladimir Grigorov

Keywords: Information society, development strategy, information and communications technologies, societal development, C4I systems.

Abstract: This article presents an analysis of the Strategy for Development of Information Society in the Republic of Bulgaria and the National Program for the Development of Information Society. It addresses issues related to the Information Society (IS) and its characteristics, principles and goals as seen by the Council of Ministers and the Ministry of Defense. The article points out the actions needed to be taken so that the goals of the IS are achieved. It also points out the importance of strengthening national security and optimizing the defense management in the establishment of IS. In this respect the article deals with issues related to developing C4I systems.

Author: **Todor Koburov**
Title: **Information Support for Decision-Making during the Kosovo Crisis**
Year of issuance: **2000**
Issue: **Information & Security. Volume 5, 2000**
Hard copy: **ISSN 1311-1493**

INFORMATION SUPPORT FOR DECISION-MAKING DURING THE KOSOVO CRISIS

Todor KOBUROV

Table Of Contents:

The establishment of a Situation Center within the Ministry of Defense and a network of situation centers connecting various ministries and institutions is a part of the Crisis Management Concept and the draft Crisis Management Act. This is going to be a continuous process, which will substantially improve the organization of the activities of different institutions in case of a crisis and will increase the level of preparedness of the Republic of Bulgaria for integration in NATO and EU.[1-3]

At the beginning we have to make some notes on the meaning of the categories "crisis" and "crisis management". There are generally accepted definitions of "*crisis*" and "*crisis management*".

> *Crisis* means "*an event with the potential for largely spreading damage, requiring rapid response measures by the government, coordination between different organizations, and sometimes - extraordinary political decisions*".

> *Crisis management* means "*a preliminary developed system of institutions and measures for prognostication of potential crises and for their prevention and handling.*"

Crises usually develop unexpectedly and sometimes resemble a time bomb. A crisis usually covers a large spectrum of negative events that may occur either on our own or on foreign territory.

Bulgaria's contribution to crisis management

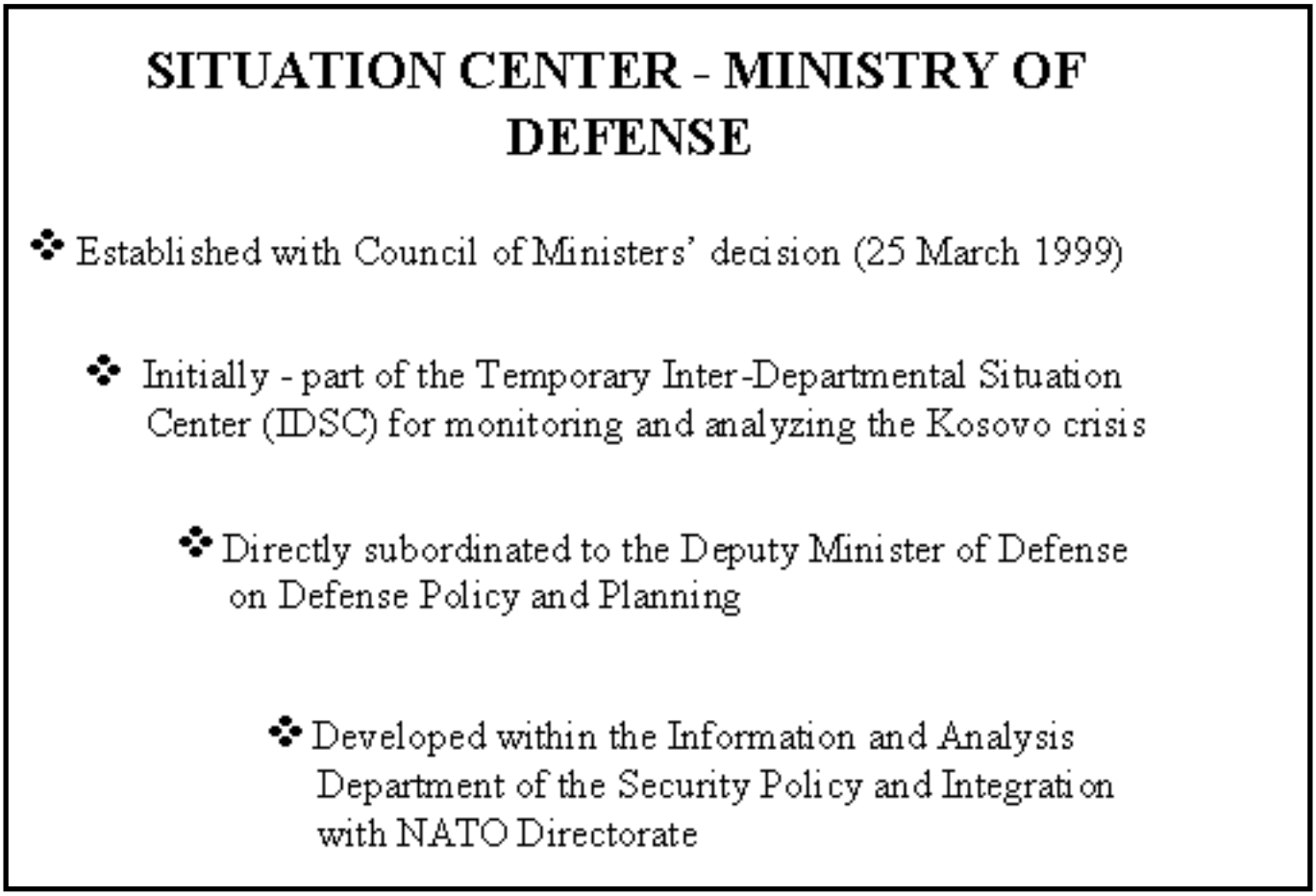
The Republic of Bulgaria must develop crisis management capabilities and a system that can adequately react to a crisis situation. Being a small country, however, Bulgaria will not initiate or conduct a crisis management process on its own. Generally, it will cooperate with international organizations like NATO, EU, UN, OSCE or a coalition led by a large nation.

It is not possible to initiate any crisis management process without *constantly monitoring and analyzing the international situation* – in the case of Bulgaria - mainly in southeastern Europe. The goal is to try to anticipate, if possible, the emergence of crises or conflicts, evaluate requests for possible participation in peacekeeping, peace-enforcement, humanitarian and disaster-relief operations, advise the policy makers on the possibilities and risks for Bulgarian participation in such operations.

The institutions that are strongly involved in this kind of activity are the ministries of foreign affairs and defense, as well as the intelligence services.

The role of the Ministry of Defense

The Ministry of Defense should concentrate on the military aspects of the international situation. The existence of a *Situation Center* within the Ministry of Defense (SC-MoD) contributes to the capabilities for a coordinated reaction to military-political crises. In certain cases and according to law, it could also react to crises of non-military character (ethnic and religious contradictions, civil disobedience with massive show of violence, increased activity of local and transnational crime structures and terrorist organizations, massive refugee flows, etc.).



The Situation Center within the Ministry of Defense was established in implementation of decision # 145/25 March 1999 of the Council of Ministers of the Republic of Bulgaria. It was designed as a segment of the Temporary Inter-Departmental Situation Center (IDSC) monitoring and analyzing the Kosovo crisis and was directly subordinated to the Deputy Minister of Defense on defense policy and planning.

SC-MoD is developed within the Information and Analysis Section of the Security Policy and Integration with NATO Directorate of the Ministry of Defense. In case of a direct threat to the security of the Republic of Bulgaria the Defense Planning Directorate, the Bilateral Cooperation and Regional Issues Directorate and the Interoperability Center of the Ministry of Defense reinforce it.

Functions of the Situation Center -MoD

The main functions of SC-MoD are as follows:

- to inform and advise the leadership of the Ministry of Defense on the development of the international situation, on possible and emerging crises and conflicts, as well as to make proposals for decisions on crisis management and conflict prevention activities;
- to coordinate the efforts of the institutions within the framework of the Ministry of Defense for purposeful collection of information related to the conflict;
- to make conclusions and to produce reports, analyses, positions and proposals for military-political and military-technical measures to guarantee the Republic of Bulgaria's national security and, thus, to assist the Minister and the Deputy Ministers in elaborating the policy of

the Ministry;

- to participate in the preparation of documents for the Minister and the Deputy Ministers of Defense for meetings of NATO, the European Union, and other international and regional forums;
- to prepare periodic documents on regional and international crises, risks of emerging conflicts, as well as on important international events, related to security and defense;
- to assist in carrying out information activities on the integration with NATO and other Euro-Atlantic and European structures, as well as on the military aspects of Bulgaria's security and defense policies (jointly with the Information and Public Relations Directorate);
- to maintain database on these issues together with the other departments of the Security Policy and Integration with NATO Directorate;
- to conduct briefings for the leadership of the Ministry of Defense;
- to collect, summarize and analyze information on the development of the situation in Kosovo and the Federal Republic of Yugoslavia, the international situation related to the Kosovo conflict, as well as on possible and emerging crises and conflicts in South-Eastern Europe.

In order to establish an efficient system for information and analyses it is necessary to use the experience of NATO member-states and the Partnership for Peace countries. At present, the Ministry of Defense of the Republic of Bulgaria has established excellent relations with the Ministry of Defense of the Kingdom of the Netherlands. It is appropriate to further develop and improve these relations.

In its studies, the SC-MoD addresses the following issues:

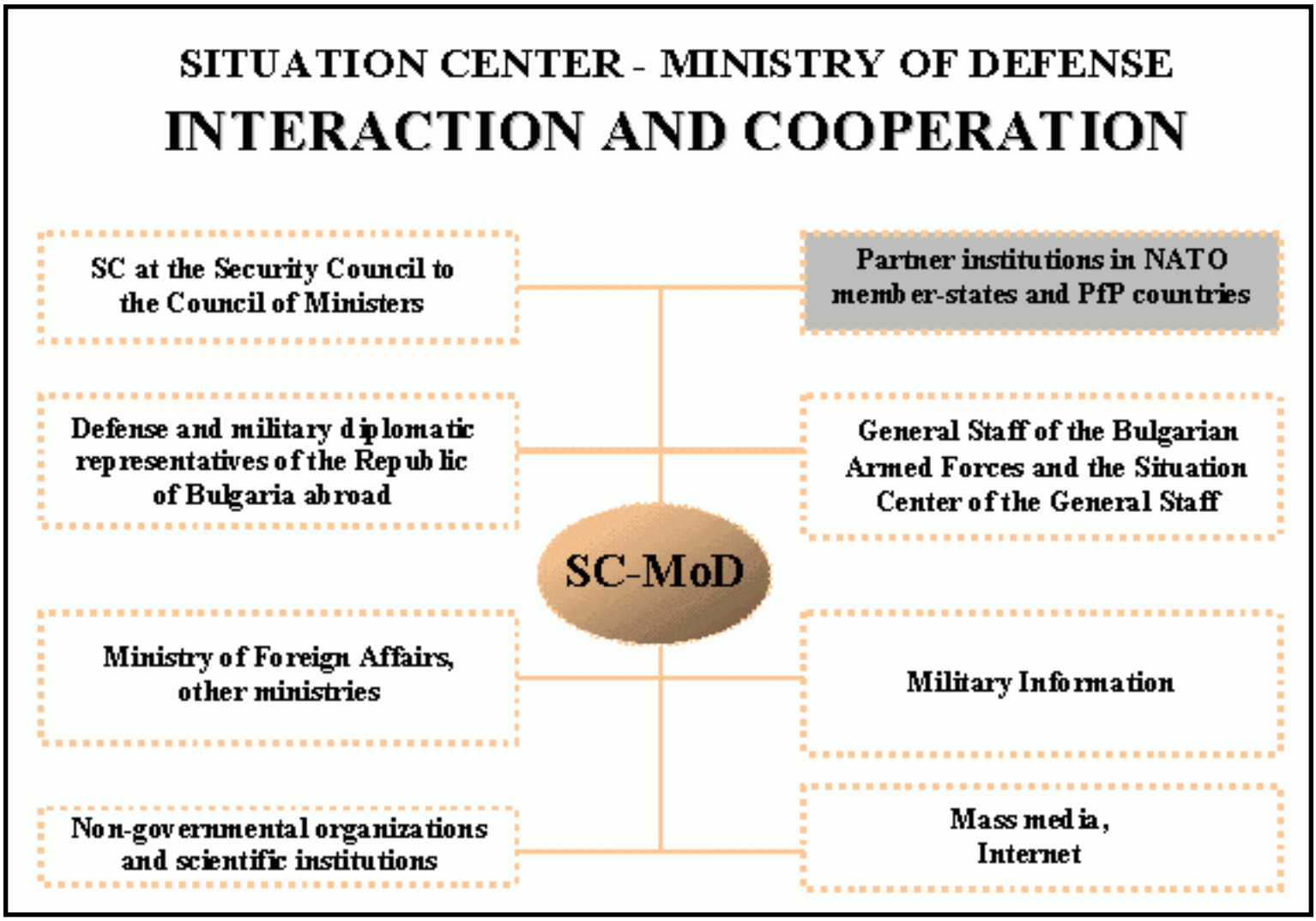
- Existing and possible crises in South-Eastern Europe, and the Kosovo crisis in particular;
- NATO: integration in NATO, participation in the Euro-Atlantic Partnership Council, Membership Action Plan, Operation Capabilities Concept, Washington initiatives - OCC, TEEP, DCI, PMF;
- European Security and Defense: cooperation with EU, the development of the Common European Security and Defense Policy, Bulgaria's participation in EU-led peacekeeping and relief operations (Petersberg missions);
- Initiatives of other international organizations dealing with security and defense issues (the United Nations, the Organization for Security and Cooperation in Europe);
- Regional Security and Defense: Meetings of the Ministers of Defense of the countries of South-Eastern Europe, the Multinational Peace Force - South-Eastern Europe, the NATO Initiative on South-Eastern Europe, the Stability Pact on South-Eastern Europe /Working Table 3, sub-table 1 – Defense and Security/, the security and defense policies of the countries of the region, bilateral relations with the countries of the region.

SC-MoD is an important segment of the Crisis Management System on national level. Taking into

account the experience of NATO member-states, and especially this of the smaller ones like the Netherlands, SC-MoD need to be staffed with highly qualified experts and analysts, and to be equipped with advanced communications means. SC-MoD has to dispose with resources for prognostication of crises, and for proposing actions for crises prevention and management. It should interact directly with and receive information from:

1. the General Staff of the Bulgarian Army and the Situation Center of the General Staff;
2. the defense and military diplomatic representatives of the Republic of Bulgaria abroad;
3. the Military Information Service;
4. the Ministry of Foreign Affairs and other ministries;
5. non-governmental organizations and scientific institutions;
6. the mass media;
7. the Internet.

It should be possible that SC-MoD cooperates and exchanges information with partner institutions in both NATO member-states and countries participating in the Partnership for Peace Program.



The experience of the Kosovo crisis

During the period 29 March - 20 June 1999 the General Reports on the Kosovo Crisis, produced by SC-MoD, had the following framework:

I. GENERAL INFORMATION;

II. RISKS FOR BULGARIA (political, humanitarian, economic, military, as well as internal security aspects and information campaign);

III. CONCLUSIONS AND PROPOSALS (which risks could lead to a threat to the national security; what should be done in order to mitigate the risks; what should be done for reconstruction of damages as a consequence of already realized threats; what new risks may emerge during the development of the situation and how to prevent them).

The framework of the General Report on Kosovo was problem-oriented and was changed in the progress of the crisis depending on the circumstances. It was focussed on the following topics:

1. Positions of the various countries and international organizations.
2. Peace initiatives.
3. Impact on Bulgaria's goals and interests.
4. Relation to the process of Bulgaria’s adherence to NATO and EU.
5. Development of the processes in NATO, the European Union, the United Nations and OSCE.
6. Evaluation of Republic of Bulgaria's position on a global and regional scale.
7. Humanitarian situation and refugees.

The SC-MoD General Report was submitted to the Minister of Defense and Deputy Ministers of Defense on defense policy and planning. It was also submitted to the Security Council at the Council of Ministers of the Republic of Bulgaria (where IDSC is attached) and was merged with the information submitted to the other teams of IDSC.

During the Kosovo crisis (the period from 29 March to 20 June 1999) the following information and analytical materials were produced:

A. GENERAL REPORTS – eighty-eight issues.

B. INFORMATION MATERIALS AND ANALYSES ON THE KOSOVO CRISIS – eleven issues on the following topics: the United Nations role; the condition of the FRY Army; possible scenarios of NATO operations; peace initiatives by 19 May plus chronology; reactions to President Milosevic's indictment by the Hague Tribunal; the Kosovo Liberation Army; strategic, economic and military

consequences of the peace in Kosovo; problems facing the peace process; comparative analysis of the military annexes to the Rambouillet and Kumanovo Agreements; the UN Security Council resolution of 10 June (summary and analysis);

C. INFORMATION MATERIAL AND ANALYSES ON OTHER ISSUES - eight issues on the following topics: Defense Capabilities Initiative; positions before the Washington NATO Summit; analyses of the Washington Summit documents (the Declaration, the Communiqué, the Strategic Concept, the Kosovo Declaration, assessments of Washington Summit of Belgium and of NATO Assistant Secretary General K.P. Kleiber, the WEU Action Plan "Europe of Defense").

Conclusions, recommendations and proposals

The Kosovo crisis showed the need to accelerate the establishment of a National Situation Center and a network of departmental situation centers for crisis management.

It is essential to establish a crisis management system based on the current legislation. The adopted Crisis Management Concept could, in principle, be the starting point for such a system. The process of legislative regulation in this field should continue with the adoption of a Crisis Management Act by the National Assembly.

The experience of the Kosovo crisis showed that the interaction between the departments, participating in IDSC, was unsatisfactory. One reason for that was the lack of a unified crisis management system. Another reason was the unclear definition of the functions and sharing of the responsibilities among various institutions - who is responsible for what and what could be expected from which institution. In many cases there was doubling of functions while one of the key issues for the national security - the political risks of the Kosovo crisis for the Republic of Bulgaria - remain practically uncovered.

The system of interaction between the institutions in case of a crisis must be worked out in advance, including clear definition of the functions and responsibilities. The principle framework of the reports and documents must also be prepared in advance allowing for changes in the course of the crisis depending on the circumstances.

In the establishment of the crisis management system serious attention must be paid to staff competence and technical equipment. In this respect, a "Vision of the Situation Center - Ministry of Defense" has to be elaborated.

References:

1. Velizar Shalamanov, "Analysis of the Threats and Synthesis of the Force Structure and Disposition," in *Proceedings of 15th AFCEA-Europe Symposium* (Brussels: AFCEA-Europe, October 1994), 59-63.

2. Stoicho Stoichev, Boris Buchinsky and Velizar Shalamanov, "Network of Situation Centers for Improved Management and Coordination," *Military Journal* 57, 6 (1994), 102-112.
3. Todor D. Tagarev, "The New Military Doctrine of The Republic of Bulgaria: Contribution of Communications and Information Technologies to Achieve National Security Objectives," in *Proceedings of the C4/NCMC International Conference* (Sofia, Bulgaria: June 1999), 7-17.

TODOR KOBUROV graduated political sciences at Sofia University in 1991. He has been working for the Ministry of Defense since 1995. He submitted his doctoral thesis in 1996 and became a doctor of political sciences at Sofia University. In the period March – September 2000 he took a specialized course in European Security on the "Count Baudisin" international program at the Peace Studies and Security Policy Institute of the Hamburg University.

BACK TO TOP

Information & Security. An International Journal
e-mail: infosec@mbox.digsys.bg

Information Support for Decision-Making during the Kosovo Crisis

Todor Koburov

Keywords: Situation Center, C3, Crisis Management, Kosovo

Abstract: The 1999 Kosovo crisis provided impetus for establishing and networking situation centers within the Council of Ministers, the Ministry of Defense and other state institutions in Bulgaria. Organizational and technological approaches were implemented to turn the network of situation centers into a valuable tool for information processing, consultations, and crisis response management at governmental level. This article describes the establishment and the functioning of the Situation Center at the Ministry of Defense during the Kosovo crisis, its interaction with related organizations, and provides recommendations for further improvement of the information support for crisis management.

Author: **Kate Starkey and Andri van Mens**
Title: **Defence Budget Transparency on the Internet**
Year of issuance: **2000**
Issue: **Information & Security. Volume 5, 2000**
Hard copy: **ISSN 1311-1493**

DEFENCE BUDGET TRANSPARENCY ON THE INTERNET

Kate STARKEY and Andri van MENS

Table Of Contents:

As the Balkans and the international community look back on more than ten years of unrest in South-Eastern Europe (SEE), many are striving to find solutions to the region's problems. One measure being contemplated is regional defence budget transparency. It is thought that if the SEE states can come to a common agreement on sharing defence expenditure information, a mutual understanding and an enhanced dialogue on security matters can be achieved. Better understanding of each others' concerns in turn would lead to increasing confidence between states, reducing military tensions among neighbours. With respect to the development of democratic institutions, transparency can furthermore enhance public debate and contribute to the efficiency of the democratic processes.

While matters of secrecy and transparency in public affairs have traditionally been of public concern,[1] today's modern technology has the potential to elevate the issue to a higher level. As Joseph Stiglitz notes:

> The end of the Cold War has provided us the opportunity […] to re-examine the role of secrecy and openness. At the same time, new technologies have provided mechanisms through which information can be more effectively shared between government and those governed.[2]

In this paper, after focusing on some issues of democracy, defence budget transparency and what they mean for security, we assess the availability of defence expenditure figures on the Internet for some European and North American countries. This is done in order to come to better understand what is available at the moment, to find out what more can be done with respect to defence budget transparency on the Internet, and ultimately to see in what way this tool can become useful in enhancing regional military cooperation and understanding in SEE.

Issues of Democracy, Defence Budget Transparency, and Security

A fundamental relationship exists between defence budget transparency and peace and security in a region. It supports the notion that democracies avoid using military means when solving disputes. The dynamic is as much internal to each state as it is external on a larger regional scale, as transparency allows for better national and international control over the government decision-making process.

Transparency in governance is a prerequisite for a sound democratic system. If democracy is a political system built on social dialogue where open discussion is fundamental to the decision-making process, then openness of information has to be its pillar. As such, transparency, underpinning the right to know, is a basic public right in a democratic society. Moreover, only transparency can lead to well-informed rational decisions. As Joseph Stiglitz further states: "It is only […] through informed discussion of the policies being pursued […] that effective governance can be exercised." The availability of information as well as the openness of the decision-making process enables experts to participate in the public debate. Basing their assumptions on accurate information, these experts can assess a situation, evaluate the alternatives, set the priorities, and recommend the best public policy available given its projected outcome. The accuracy of their projections can be expected to be proportional to the information available since transparency is key to correct policy evaluation. In fact, openness of information creates a realistic opportunity for timely policy adjustments when forecasting errors occur. Thus democracy relies on openness of information as well as public and expert control. While public debate insures that people are talking, the availability of information guarantees that everyone is talking about the same thing. Democracy is a system of checks and balances, of consideration and reconsideration: it is a decision-making process, a process that is fundamental to the sound planning of public affairs.

The planning, programming, and budgeting system (PPBS) used in the United States for defence budget development and presently being introduced in the Bulgarian Ministry of Defence, relies on a defence programming cycle of this nature.[3] A typical PPBS cycle consists of an initial planning phase, in which the security environment, as well as national interests and threats are analysed in order to determine the tasks, the composition, and the structure of the armed forces. Considering these imperatives, programs are developed. The program, a form of business plan, identifies the concrete objectives to be met. It is a crucial link in the cycle as it works to relate the identified objectives to the financial resources. In this way, PPBS parts with the practice of allocating resources according to the stated needs and instead looks to plan and program according to given and forecasted budgetary constraints. Hence, it is important that the programs are developed on a priority basis, where the most immediate needs for the armed forces are met. Risk assessments dealing with the consequences of not meeting a given objective can be used for setting the priorities. Completing the cycle in the end is a performance measurement phase during which the ministry in particular and society as a whole can

determine to what extent the objectives have been met at the end of the year. An efficient distribution of resources can thus be achieved:

> [B]eing introduced with the aim to increase effectiveness of defence resource management, defence programming is an important element of civil-military relations and, potentially, an important driving force for the establishment of effective democratic control over the armed forces.[4]

The different stages of the cycle provide an opportunity for, and are indeed submitted to, public scrutiny through public discussion, expert involvement and parliamentary ratification. In relation to defence policy and military expenditures in South Eastern Europe (SEE), public as well as expert influence could elevate the decision-making process beyond emotional value-loaded historical considerations.[5] As well, accurate threat assessments could in turn lead to the restructuring of armed forces and defence expenditure reductions. The money saved could potentially be used in the socio-economic sphere, which would make sense security-wise, as economic development would undoubtedly lead to greater social stability. On the contrary, excessive defence expenditures might lead to greater unrest. As Paul George points out:

> We know from past experience that excessive military expenditure can increase economic insecurity by reducing the availability of resources that could be invested more beneficially in other sectors. Economic insecurity can then become a potential source of internal instability thereby leading to a vicious circle in which further security expenditure is required as governments strive desperately to contain unrest. Nor do internally generated military expenditure increases easily remain confined to a single state. As a country increases its defence spending to contain domestic instability, alarm bells ring in neighbouring countries and regional military spending levels tend to rise in response. Inevitably, this broadens the negative impact of increases in the unproductive use of scarce resources and reduces regional opportunities for investment in urgent social sector priorities. It also perpetuates the cycle of instability and decreases the overall security environment.[6]

Of course, military cutbacks in one country are contingent on similar cutbacks in neighbouring countries, and it thus comes down to knowing what the others' defence priorities are.

Diplomatically, defence budget transparency based on planning and programming is an important confidence-building tool between neighbouring countries.[7] Transparency in the budgeting process, part of which is concerned with risk assessments and evaluations of the security context, enables a country to indirectly influence another's defence decision-making process. As such, it provides one with the opportunity to correct another's strategic concept (possibly by clarifying its own), and to ask specific questions related to the defence policy (procurement, exercises, restructuring, etc.) "[As] the general lack of accountability and transparency in defence budgeting can […] feed concerns about the size, capabilities and intentions of a country's armed forces", writes Paul George, "[g]reater transparency will draw attention to military spending and reduce the potential for uncertainty and misunderstanding that lead to conflict."[8] In the end, it creates a greater feeling of security.

Overall, transparency facilitates control over defence spending, reducing the possibility of excessive expenditures. As a result, more money can be channelled to socio-economic development. In this way, transparency can both reduce militarism, in itself a conflict-enhancing factor, and moderate socio-economic tensions. In essence transparency leads to dialogue and well-informed, rational decisions.

Defence Budget Transparency on the Internet

Effective civil control over the government decision-making process depends both on transparency during the budgeting process and on transparency in terms of free access to the budget as it is voted by parliament. One is not distinct from the other. If experts are to participate in discussions, they need to be informed through access to previous budgets. More importantly, if foreign governments are to be informed, they would most likely want to have the same opportunity for comparison and will appreciate having access to the official defence expenditure figures and the nature of these expenditures. Modern technology provides governments and defence ministries access to such data through the Internet, a relatively quick and inexpensive research tool offering immediate results, provided the information is available.

The following report looks into the availability of the above-mentioned information. It was compiled to provide a baseline for measuring the progress with respect to budget transparency in the future. The results varied, from countries that presented very detailed and informative backgrounds on their military spending, to other countries that only provided a brief background and a couple of figures, if any.

The research was conducted by dividing the countries into three sections. This was mostly done with the intention of comparing countries of similar backgrounds with one another so that any discrepancies between countries as a whole would not be too large. The following sections were created for the purpose of comparative research:

- South Eastern European countries (countries participating in the South-Eastern Defence Ministerial and the Multi-National Peace Force South-Eastern Europe /MPFSEE/, as well as Stability Pact members)
- Other Central and Eastern European countries
- Western European and North American countries

The findings come from the English versions of the countries' defence and finance ministries' websites (in some cases the general governmental site was consulted). Choosing the English language is a normative consideration, which should be kept in mind when reading this document. As a now widely recognized diplomatic language, our focus on the availability of English information seems nevertheless to be a legitimate choice, especially if one considers defence budget transparency as a diplomatic tool for avoiding armed conflict. One should not conclude however, that the lack of budgetary information on the English sites illustrates a lack of openness on the part of either the Ministry of Defence or the Ministry of Finance of the respective countries.

Country Reports

South Eastern Europe (MPFSEE and Stability Pact members)

Albania

None of the relevant Albanian institutions can be reached through the NATO-site, which lists all the NATO partner countries and links to important state institutions (i.e. Parliament, Head of State, Government, Ministry of Defence, Ministry of Foreign Affairs, and the Ministry of Finance). If such pages do exist however, then it should be noted that they are hard to find as we unsuccessfully searched the Internet with some of the more frequently used search engines.

Bosnia and Herzegovina

As in the case of Albania, there appears to be no relevant information for Bosnia and Herzegovina available on the Internet.

Bulgaria

Defence budget information for Bulgaria is scarce on the Internet. The Ministry of Finance at http://www.minfin.government.bg/www/index.html and the Government at http://www.government.bg barely mention defence, let alone defence expenditures. The Ministry of Defence at http://www.md.government.bg has some indirect budget information in its executive summary of the *Plan for Organizational Development of the Ministry of Defence by the Year 2004* as it covers capabilities restructuring, infrastructure restructuring and defence budget restructuring without providing explicit expenditure figures. There seems to be progress however as the Bulgarian Government published, while we were finalizing the current report, the English version of the *Annual Report on the State of National Security of the Republic of Bulgaria in 1999* (Sofia, June 2000) at http://www.government.bg/eng/oficial_docs/index.html. In five of its appendixes it contains information on defense and security related expenses in terms of functions and operations. The report points out that 656.9 million levs equal to 2.88 % of the GDP or 6.44 % of the state budget were spent on defence. Of that amount 580.6 levs, or 2.55 % of the GDP, made up the budget of the Ministry of Defence. The report gives a cross-section of the other defence and security related expenses, as well as their distribution in terms of 'costs', 'wages, social security, etc.' and 'investments.' It is expected that detailed distribution of the defence budget will be made available through the Internet with the publication of the first *Annual Report on the State of Defence and the Armed Forces of the Republic of Bulgaria*.

Croatia

Croatia has very little budgetary information on the Internet, especially pertaining to the defence budget. The English version of the web page of the Government of Croatia can be found at http://www.vlada.hr/english/contents.html. While there is no budget information here, there are links to the different ministries. The Ministry of Defence is at http://tomislav.morh.tel.hr, but the site is under construction and has been for a while. Thus the only hint of any military budget information is found on the site of the Ministry of Finance at http://www.mfin.hr/index_eng.htm. This site presents

very informative monthly statistical reviews prepared by the Macroeconomic Analysis and Forecasting Department of the ministry and going back to 1995. The latest one, the June 2000 issue (no. 56), compiles figures concerning the countries defence expenditures. Table 3A gives the Budgetary Central Government Expenditures by Function. The table shows expenditures for Defence Affairs and Services have gone down from 6990659 Croatian crowns (HRK) in 1997 to the planned 4786388 HRK for 2000. The share of the defence expenditures in the State Budget has thus fallen from 20.3% in 1997 to 13.1% in 2000.

Former Yugoslav Republic of Macedonia

The Republic of Macedonia has an English version of its Ministry of Defence website at http://www.morm.gov.mk/eng/mo_e.htm. While the defence budget cannot be found at this site, there is however a copy of the 1998 *White Paper of the Defense of the Republic of Macedonia*. Chapter 4 of this White Paper is dedicated entirely to budgetary issues. It contains information on the defence budgets for 1997 and 1998, on the further development of the defence budget, and a projection until 2008 of the defence budget. In 1997, the Ministry of Defence obtained $60,171,406 US from the State budget or 2.23% of the GDP and 8.96% of the total budget. For 1998, similar figures were projected with a budget covering up to 8.56% of the total budget, equivalent to 2.27% of the GDP with the total amount of expenditures projected at $70,911,964 US.

Between 1997 and 1998, 52.65% (1997) and 54.75% (1998) of the expenditures were general *Defence Resources, and Personnel* expenditures accounted for the other 47.35% and 45.25% respectively. Considering economic projection until 2002, the defence budget will grow to $99 million US from the $70.91 million US in 1998. At the same time however the participation of the defence budget in the GDP will fall from 2.27% in 1998 to 2.1% in 2002. For the long-term, the defence budget is expected to grow to $102 million US in 2008.

Greece

The Greek governmental websites provide the outside observer with close to no information. Websites for the Ministry of Defence (http://www.mod.gr/english/index.htm), the Prime Minister's Office (http://www.primeminister.gr/index_en.htm) and the Ministry of Finances (divided in two sections: General Accounting Office at http://www.mof_glk.gr and General Secretary of Information Systems at http://www.gsis.gov.gr) do exist, but while some of them have English versions most of the relevant information is in Greek. The Ministry of Defence's web page has a link to the Greek White Paper, a link however, that is not active.

Italy

As in the Greek case, it is difficult for the outside observer to obtain any information pertaining to the Italian defence budget and the budgeting process as the official governmental websites are in Italian only (Ministry of Defence at http://www.difesa.it, the general government site at http://www.palazzochigi.it and the Ministry of Finance site at http://www.finanze.it).

Romania

Romania has two sources for defence budget information. The first can be found at the English language version of the Romanian Ministry of Defence's website at http://www.mil.logicnet.ro/old/0.htm. One section on this site deals in particular with the Defence Budget. It contains charts and graphs that show the evolution of the defence expenditure between 1990 and 1998. It appears these expenditures have fallen from $1337.49 million US in 1990 to a little more than $707 million US in 1997. In 1997, the Defence Budget accounted for 8.6% of the State budget and for some 1.77% of the GDP. In 1998 these figures were respectively 7.77% and 1.68%. According to another chart, $205,54 million US were spent on personnel expenditures in 1997, whereas $164,91 million US were used for material expenditures and $163,87 million US for Capital Investments.

The Romanian Ministry of Finance (http://www.mfinante.ro/menua.htm), in turn, has a monthly bulletin on its website with, amongst other things, the General Consolidated Budget, the State Budget and the accompanying charts. According to the figures concerning the State Budget of 1999, defence expenditures were to attain 8529,8 billion lei.

Slovenia

Slovenia's Ministry of Defence has an English version web-site at http://www.mo-rs.si/mors/eng/index.htm. It covers subjects related to the Ministry of Defence through one link and the Slovenian Armed Forces through another. The Ministry of Defence section has no specific budget information. Only in passing can some information be obtained, notably in a document entitled *Defence System* covering aspects related to the national security, the defence system, and the military duty and service. The final sections of this document address the issue of planning: Defence Planning, Force Planning, Combat Readiness Planning and Operational Planning. Within these sections one can learn about the Slovenian planning process and methodology. Basic defence planning documents are thus adopted by parliament. Overall, three defence planning perspectives exist: a long-term plan covering 10 years or more, a medium-term plan covering 5 years and a short-term plan covering the fiscal year. In 1999, approximately US $315 million, close to 1.5% of GDP, were spent on the implementation of these plans. Half of these financial resources covered the personnel costs (salaries, allowances and pensions), 22.3% of the money went to operational and maintenance costs, and 27.6% were intended for procurement. Only 0.1% was put aside for research and development.

The Armed Forces site, in turn, has more specific information about the make-up of the Slovenian armed forces. This information is found in the two documents entitled *Force Composition* and *Armament*.

Turkey

Turkey has two official sites related to military affairs: the Ministry of Defence at http://www.msb.gov.tr/bakan/bakan.htm and the Armed Forces at http://www.tsk.mil.tr. While the Ministry of Defence site is only available in Turkish, the Armed Forces site also has an English language version, which unfortunately was out of order during the time of the reported research.

Although there is an English welcoming message on the home page, the Ministry of Finance site at http://www.maliye.gov.tr is in Turkish as well. Furthermore, it is still under construction.

Other Central and Eastern European Countries

Belarus

There appears to be no relevant information on the military budget of Belarus on the Internet as there are no Ministry of Defence or Ministry of Finance websites.

Czech Republic

The English versions of the Czech Ministry of Defence site at http://www.army.cz/english/index.htm, the Government site at http://www.vlada.cz/1250/eng/vlade/vlada_clenove.htm, and the Ministry of Finance site at http://www.mfcr.cz/scripts/hpe/default.asp have no specific military budget information. The government has some related information on their site in a document stating its policy. Chapter 4.4 covers subjects related to internal security, defence, and foreign policy. Taking into consideration its country's accession to NATO, the Czech government promises to adopt basic documents relating to the security, defence and military strategy. Moreover, it plans to "implement the commitment to increase military spending gradually by 0.1% annually to reach 2% of GDP by the year 2000."

The Ministry of Finance provides some government financial statistics, including very basic expenditure figures. An analysis of these figures shows that Czech defence expenditures grew from 27,621 billion Czech Crowns (CZK) in 1994 to 33,936 billion CZK in 1999. Military capital expenditures went up from 5,945 billion CZK in 1995 to 9,415 billion CZK in 1999.

Estonia

The Estonian Ministry of Defence website is found at the address: http://www.mod.gov.ee where the only English link that exists provides the viewer with the Annual National Plan for implementation of the country's Membership Action Plan. Within the National Plan there is a brief paragraph addressing budgetary issues. This paragraph states that Estonia will increase its defence expenditures to 2% of the GDP by the year 2002, following the schedule of 1.6% in 2000, 1.8% in 2001, and 2% in 2002. This increase will focus on the establishment of an adequate military infrastructure in the sphere of military training and the quality of life of personnel. The Annual National Plan also states that "the overall objective of budget planning is to ensure complete transparency between the resources needed, political guidance and the planned goals."

Hungary

The Hungarian Ministry of Defence website is located at http://www.h-m.hu/mod. There is no specific budget information available. Within the Ministry's organizational chart, there is a section entitled

MoD Budget Monitoring but no description follows. The Ministry of Finance website, which can be found through the governmental home page at http://www.meh.hu/default.htm, does not have any budgetary figures related to defence spending published in English on its site either.

Latvia

The Latvian Ministry of Defence website is located at http://www.mod.lv and although there is an icon for English viewing, the link is not in order. There is an English version of the Ministry of Finance website however (http://www.fm.gov.lv/05sak/05sak_a.htm), but it has no defence expenditure information.

Lithuania

The Lithuanian Ministry of Defence website is located at http://www.kam.lt/english. At this address there is a link to the 1999 White Paper. Within the White Paper there is a brief section on the budget. This section addresses such issues as the guidance for the defence budget, figures within the defence budget itself, military construction and procurement (extra-ordinary expenditures), and 'ordinary expenditures'. The Lithuanian government plans to increase defence spending through the following schedule: 0.8% of the GDP in 1997, 1.3% in 1998, 1.70%-1.75% in 2000, and 1.95%-2.0% in the year 2001. In 1999 the defence budget was expected to be approximately 724 million Lt. ($181 million US).

The above seems to be all the information available as the English language Ministry of Finance website at http://www.finmin.lt/fmhomeen.htm has budget information, but no military expenditure information.

Moldova

The English website address for the Moldavian Ministry of Defence is http://www.moldova.md/ro/government/oll/DEFENSE/index.htm. There are presently only four links on this page, none of which are related to budget information or expenditures. The Ministry of Finance website at http://www.moldova.md/en/government/index.html doesn't provide any defence budget information either.

Poland

The Polish Ministry of Defence website is located at http://www.wp.mil.pl/glowna.html, but unfortunately the English language link is not active. This is also the case with the "Budget" link on the English Ministry of Finance website at http://www.mofnet.gov.pl/ministry/index.shtml.

Russia

Russia does not appear to have a Ministry of Defence website as this ministry is not mentioned on the special links page of the Russian Ministry of Foreign Affairs, where the Internet addresses of

governmental departments and agencies are listed. On the other hand, the Russian federation is represented online with a Ministry of Finance website at http://www.minfin.ru. This site is in Russian only but has a few links to English pages. One of these links, entitled *Information on Fiscal Sector presented by Economic Expert Group*, leads to the Economic Expert Group of the Ministry of Finance of the Russian Federation website at http://www.eeg.ru. There is a table on this site giving the figures pertaining to the Federal Budget Execution. At the time of this research, it compared the budget execution for the months of January through May of 1999, with the budget execution for the same months of 2000. Defence expenditures for the first five months of 1999 were 32,5 billion Russian Roubles (RUR) or some 2.2% of GDP. During the same months this year, defence expenditures went up to 70,1 billion RUR, or some 2.9% of GDP.

Slovakia

The Slovakian Ministry of Defence website is located at http://www.mod.gov.sk but is presently unavailable. There is however some defence budget information available on the Ministry of Finance site at http://www.finance.gov.sk. Through the link *State Budget*, it is possible to obtain the state budget expenditures figures for 1999. Defence budget expenditures, 20,7 billion Slovak Crowns (SKK), are listed as public consumption of the state under current expenditures which, at 178,5 billion SKK, account for almost 92% of the total state expenditures (the rest being capital expenditures).

Ukraine

Ukraine appears to have a Ministry of Defence website at http://www.dod.niss.gov.ua, but when entrance is requested, the server seems not to be operating. The Ministry of Finance site is located at http://www.minfin.gov.ua. This site includes a button for an English version, but at the time of the research it was not activated.

Yugoslavia

Yugoslavia does not appear to have a website for its Federal Ministry of Defence or its Ministry of Finance as such sites cannot be found with the help of elementary Internet surfing.

Western Europe and North America

Canada

The Canadian Department of National Defence website, at http://www.dnd.ca, provides basic budgetary information. The budget information is found within the policy section of the site, at http://www.dnd.ca/admpol/docs_e.htm, and provides 1999/2000 estimates in defence spending. Some of the details include elaboration on spending by maritime forces, land forces, air forces, as well as charts with a historical-comparative overview. Links are also provided to the Ministry of Finance website at http://www.fin.gc.ca, where full viewing of the 1998, 1999, and 2000 budgets is possible. For the 1999-2000 fiscal year, defence budget was apportioned as follows: 67.8% of the budget was allotted to personnel, operations and maintenance expenditures, 19.7% to capital expenditures, 5% to

grants and contributions, and 7.1% to pensions and benefits plans. The Department of National Defence budget for 1999-2000 is $10.515 billion (including revenues, but less transfers), up from $10.165 billion the previous year. Defence as a share of Gross Domestic Product will continue to hold at just above the one percent threshold.

Finland

The Finnish Ministry of Defence website is located at http://www.vn.fi. Here, several English-language charts are available that outline defence spending in Finland. For example, in 1999, the share of defence spending from the total state expenditure was 4.82% and the 1999 budget proposes defence spending at 1.3% of the GDP. The site also offers a chart detailing the division of defence spending in 1999. Of a total of 9,028 million FIM, 3490 million were spent on procurement, 3402 on payroll, 775 on other expenditures, 761 on real estate, 530 on the upkeep of transcripts, and 70 on peacekeeping. The Ministry of Finance website at http://www.vn.fi/vn/vm/english/mof.htm does not provide any additional information.

France

The French Ministry of Defence website (http://www.defense.gouv.fr) presents only the evolution of the defence budget in English. This evolution, which compares defence spending with countries such as Germany, the United States, and Great Britain as well as analysis through other comparative measures, is predominantly done in graph form with very little text. These charts can be found at the Internet address: http://www.defense.gouv.fr/sga/budget/indexb.htm. The Ministry goes into slightly more detail in French. One chart presents defence spending with respect to the state budget and the GDP, where defence spending steadily decreases as the two others gradually increase. The percentage of GDP spent on defence by the French government is also presented alongside that spent by the UK, the United States, and Germany. In 1997, France spent 2.93% of its GDP on defence, and 2.71% in 1999.

Germany

The German Ministry of Defence website (http://www.bundeswehr.de) is predominantly in German with some extracts in English. Within the English extracts there is a section entitled *Bundeswehr Planning - Capabilities, Structures and Resources,* in which some budgetary planning and expenditures are briefly outlined. The information provided stresses the German commitment to German unification, which "will absorb large amounts of funds for the foreseeable future." As a result, the defence budget has been placed at a lower priority than German unification. From the fiscal year of 1991, when the first all-German budget was introduced, until the fiscal year of 1994, defence expenditure was cut by approximately 6.4 billion DM (12 percent). The 1999 defence budget amounts to around 47.52 billion DM or approximately 10.2% of total federal expenditures.

Great Britain

The British Ministry of Defence website (http://www.mod.uk) has made a copy of its *Annual Report*

of Defence Activity available in Adobe format. As well, it also has a copy of *Expenditure Plans 99/00 to 00/01* and *Expenditure Plans 00/01 to 01/02* in Adobe Format. *Expenditure Plans 00/01 to 01/02* provides details in the area of the MoD's cash base with the total value of fixed assets at £65 billion. A detailed breakdown in cash plans studies the expenditures of the General Officer Commanding (Northern Ireland), Chief of Joint Operations, Chief of Defence Logistics, Defence Systems Procurement, Retirement pay, pensions and other payments to Service personnel, etc. The document also addresses the trends in cash spending. In 1999/2000, cash provision was valued at £22,863 million with spending at 2.6% of the GDP. The *Expenditure Plans* go into further detail with respect to Contingent Liabilities, Contingent Liabilities in Excess of £100,000, Appropriations in Aid, Public-Private Partnerships, Long Term Projects, Ship Procurement, Refitting, and Repair, and Exports of Defence Equipment.

Complete budget information, with the State Budgets from 1994 onwards, can be found at the Her Majesty's Treasury website at http://www.hm-treasury.gov.uk.

The Netherlands

The English version of the Dutch Ministry of Defence website at http://www.mindef.nl/english/index.htm has no budgetary information. One interesting document on the site is the *Framework Memorandum for the 2000 Defence White Paper*. However, as a starting point for broader discussion leading to the publication of a Defence White Paper outlining Dutch defence priorities for the coming decade, it has no specific budget information. It only gives a broad picture of the financial constraints upon the national military in a chapter entitled *Financial Aspects*. Thus, we learn that the Ministry of Defence is facing cutbacks in its yearly budget, that it plans on investing some more money and that it hopes to finance these investments through restructuring of its armed forces.

We learn more about the defence budget cutbacks on the Ministry of Finance website at http://www.minfin.nl/Minfinuk.asp?blnNews_UK=-1. In a document entitled *The Abridged Version of the Budget Memorandum 2000*, to be found through the *Budget* link, the Dutch Ministry of Finance notes that defence expenditures for 1999 and 2000 reach some 13.8 billion Dutch guilders (NLG), or some 6.26 billion euros. These expenditures have thus been cut by NLG 0.4 billion.

United States

The defence page for the U.S. Department of Defense can be found at http://www.defenselink.mil. Although the actual budget does not appear to be available through Defenselink, one section of the site does explore *DoD's Slice of the $*. Within this section, several issues are addressed, including: breakdown of the budget, the budget by component, DoD estimate payroll, contracts, and grants by state/area, procurement dollars, top defence contractors, and a research development, test, and evaluation program. Another document available through the Internet is the *President Clinton's Fiscal Year Defense Budget*.

Conclusions

The Internet appears to be a powerful tool for researching military budgetary figures. Although the availability varies from country to country, a fair bit of relevant information can be gathered to answer immediate questions related to military budgets. There are drawbacks however to using the Internet for this type of research. First, not everybody has the means to put information on the Internet for public consumption. Thus, one might erroneously conclude that a country has not made its budget public, when in fact it simply has not been made available on the Internet. Likewise, the technology used by the person looking into the information can also be an obstacle to efficient access to the information, which has been made available on the Internet. Using the facilities made available to us at the Bulgarian Ministry of Defence, we noticed for example that certain files were difficult, if not impossible, to download. Secondly, in terms of language, not all Ministries of Defence translate their entire sites into English. Often only excerpts are made available. Thirdly, reports with complete figures and details are rare. Instead, excerpts are most often the only information available, and comparing defence budget excerpts from one country with those of another does not make for comprehensive and convincing research.

The research also provides further conclusions. There does not appear to be a NATO standard for the way in which member countries should present military budget information. This does not give NATO-aspiring countries any sort of indication of what military budget transparency through the Internet should consist of or how it should be presented. Although it would appear obvious that the percentage of the GDP is a fairly basic starting point, some NATO member countries have not made this information available on their Internet sites. Incidentally, there are a number of non-NATO countries that have made this information very readily available, in the English language.

Thus, as a preliminary step into the research of military budget transparency issues, Internet research provides a constructive and clear framework. It should always be kept in mind though, that there are some constraints to this type of research, which can directly affect the findings and resulting comparisons. Full defence budget transparency that can lead to better civil and international control, and ultimately to a higher degree of regional security, is not yet a fact of life when it comes to the information made available on the Internet. Consequently, the Internet, if not used properly, could become not a tool for democracy, but on the contrary a hindrance to the democratic processes where information remains incomplete and possibly incomprehensive.

There is a danger that full reliance on the Internet to provide the people with information could put the citizen at risk of losing ground against ever more technocratic and complex state institutions. When analysing democracy in America, Alexis de Tocqueville observed that the system was successful because of its federal nature and the existence of pressure groups, in other words, because of the existence of a formal circuit of checks and balances of the central governmental institutions. According to the French political philosopher, the individual alone is helpless against the state.

Drawing a parallel with the feudal societies in Europe, where the aristocracy exercised control over the sovereign monarch, de Tocqueville was worried about the anti-democratic effects of the French Revolution. Without the powerful aristocracy to curb its power, he thought the new French republican state would become an ever more authoritarian institution imposing its will on the lonely and alienated citizen. Likewise, a modern society without civil organizations to defend the particular interest of the citizens would tend to be authoritarian, as the state would be freed of all social control.

As a matter of fact, these civil organizations tend to have more resources (time, money and expertise) than the individual citizen to keep an eye on and analyse public policy.

As the democratic attributes of the Internet seem to be growing every day, the fundamentals of de Tocqueville's conclusions appear to be ever so pertinent. If the citizen is abandoned in the global village, forced to surf the Net by himself and without the guidance and expertise of civil organizations, he will find himself isolated when facing governmental institutions, information and decisions.

Thus it is important, in the name of the democratic process, to come to a balanced conclusion of both the advantages of the Internet as a tool for rendering information more available and the expertise of national or international governmental or non-governmental organizations as interpreters of this information. With respect to the defence budget transparency through the Internet and its effects on regional security, governments appear to need expert technical help in order to provide the relevant budgetary information.

Furthermore, they seem to need guidelines as to what should be made available and where. Such guidelines, if internationally determined, will put the different governments at ease when providing their information, knowing that the others will be doing it as well. The creation of some kind of regional institution concerned with setting the guidelines and gathering and interpreting the information appears thus to be a prerequisite to achieving sound defence budget transparency through the Internet in SEE.

Noticing that "every developing region has some form of regional institution that could serve as a collection point and repository for defence spending information" and that "each developing region has one or more core states which have developed, to some degree, greater transparency in defence budget matters", Paul George considers that "a greater effort should be put into developing regional, or sub-regional, data bases on defence spending, [as] this effort should be undertaken at the regional level, using local resources as much as possible." "A smaller, localized, system of reporting on defence spending would provide regional states with a larger stake in the security outcome of the process and would encourage greater reporting compliance."[9]

Appendix: A List of the Internet Addresses Mentioned in the Article

Bulgaria

- Government - http://www.government.bg

- Ministry of Defence - http://www.md.government.bg

- Ministry of Finance - http://www.minfin.government.bg/www/index.html

Canada

- Department of National Defence - http://www.dnd.ca

- Department of National Defence: Defence Policy - http://www.dnd.ca/admpol/docs_e.htm

- Ministry of Finance - http://www.fin.gc.ca

Croatia

- Government - http://www.vlada.hr/english/contents.html

- Ministry of Defence - http://tomislav.morh.tel.hr

- Ministry of Finance - http://www.mfin.hr/index_eng.htm

Czech Republic

- Government - http://www.vlada.cz/1250/eng/vlade/vlada_clenove.htm

- Ministry of Defence - http://www.army.cz/english/index.htm

- Ministry of Finance - http://www.mfcr.cz/scripts/hpe/default.asp

Estonia

- Ministry of Defence - http://www.mod.gov.ee

Finland

- Ministry of Defence - http://www.vn.fi

- Ministry of Finance - http://www.vn.fi/vn/vm/english/mof.htm

Former Yugoslav Republic of Macedonia

- Ministry of Defence - http://www.morm.gov.mk/eng/mo_e.htm

France

- Ministry of Defence - http://www.defense.gouv.fr

- Ministry of Defence: Defence Expenditure Charts -

http://www.defense.gouv.fr/sga/budget/indexb.htm

Germany

- Ministry of Defence - http://www.bundeswehr.de

Great Britain

- Ministry of Defence - http://www.mod.uk

- Her Majesty's Treasury - http://www.hm-treasury.gov.uk

Greece

- Prime Minister's Office - http://www.primeminister.gr/index_en.htm

- Ministry of Defence - http://www.mod.gr/english/index.htm

- Ministry of Finance: General Accounting Office - http://www.mof_glk.gr

- Ministry of Finance: General Secretary of Information Systems - http://www.gsis.gov.gr

Hungary

- Government - http://www.meh.hu/default.htm

- Ministry of Defence - http://www.h-m.hu/mod

Italy

- Government - http://www.palazzochigi.it

- Ministry of Defence - http://www.difesa.it

- Ministry of Finance - http://www.finanze.it

Latvia

- Ministry of Defence - http://www.mod.lv

- Ministry of Finance - http://www.fm.gov.lv/05sak/05sak_a.htm

Lithuania

- Ministry of Defence - http://www.kam.lt/english

- Ministry of Finance - http://www.finmin.lt/fmhomeen.htm

Moldova

- Ministry of Defence - http://www.moldova.md/ro/government/oll/DEFENSE/index.htm

- Ministry of Finance - http://www.moldova.md/en/government/index.html

The Netherlands

- Ministry of Defence - http://www.mindef.nl/english/index.htm

- Ministry of Finance - http://www.minfin.nl/Minfinuk.asp?blnNews_UK=-1

Poland

- Ministry of Defence - http://www.wp.mil.pl/glowna.html

- Ministry of Finance - http://www.mofnet.gov.pl/ministry/index.shtml

Romania

- Ministry of Defence - http://www.mil.logicnet.ro/old/0.htm

- Ministry of Finance - http://www.mfinante.ro/menua.htm

Russia

- Ministry of Finance - http://www.minfin.ru

- Economic Expert Group - http://www.eeg.ru

Slovakia

- Ministry of Defence - http://www.mod.gov.sk

- Ministry of Finance - http://www.finance.gov.sk

Slovenia

- Ministry of Defence - http://www.mo-rs.si/mors/eng/index.htm

Turkey

- Ministry of Defence - http://www.msb.gov.tr/bakan/bakan.htm

- Armed Forces - http://www.tsk.mil.tr

- Ministry of Finance - http://www.maliye.gov.tr

The United States

- Ministry of Defence - http://www.defenselink.mil

Ukraine

- Ministry of Defence - http://www.dod.niss.gov.ua

- Ministry of Finance - http://www.minfin.gov.ua

References:

1. Joseph Stiglitz, *On Liberty, the Right to Know, and Public Discourse: The Role of Transparency in Public Life*, Oxford Amnesty Lecture (Oxford, U.K., 27 January 1999). Available also at http://www.worldbank.org/html/extdr/extme/jssp012799.htm.
2. Stiglitz, *On Liberty, the Right to Know*.
3. Todor Tagarev gives a comprehensive view of the programming cycle presently being introduced in the Bulgarian Ministry of Defence and its implications for civil-military relations in Todor Tagarev, "Defence Programming – Crucial Link in Civilian Control," to appear in *Balkan Security and Defence Policy Modernisation* (Sofia: University Publishing Stopanstvo, 2000). The paper was presented at an international seminar under the same title in Ribaritsa, Bulgaria, on May 24-27, 2000.
4. Tagarev, "Defence Programming."
5. Tilcho K. Ivanov, *Confidence and Security in the Balkans: The Role of Transparency in Defence Budgeting* (Sofia: Institute for Security and International Studies, Research Report 6, 1996). Available in full text at http://www.isn.ethz.ch/isis/Publications/ . The author emphasises that irrational thinking is an important determinant of Balkan security today: "The irrational factors are connected with the human feelings, fears, hopes and perceptions. They have a predominant psycho-emotional character. Ethnic, religious, socio-cultural and other motives induce the people to act in one or other way. War is born by fear. It is difficult to describe

the mechanisms of this relationship, but it is out of doubt that the irrational factors are decisive for the Balkan security."

6. Paul George, "Defence Expenditures in the 1990s: Budget and Fiscal Policy Issues for Developing Countries", International Conference on *Converting Defence Resources to Human Development*, Bonn, 9-11 November 1997. Available at http://www.bicc.de/general/events/devcon/george.html.
7. Ivanov, *Confidence and Security in the Balkans.* Tilcho Ivanov writes: "[A]s the budget is a message to our neighbours about the defence goals and the ways to achieve them [and] if the welfare of the citizens is a government concern, then the resources used for security matters are an element of international relations and they influence directly the confidence and the good neighbourly relations between states." Furthermore, he writes, "acceptance of the military planning standards inherent to contemporary society is a means for restraining sudden changes of intentions and for giving clear signals about the forming of threats to security."
8. George, "Defence Expenditures in the 1990s."
9. George, "Defence Expenditures in the 1990s."

KATE STARKEY holds a Bachelor's degree in North American Studies from McGill University, Montreal, Canada. E-mail: katestarkey@hotmail.com.

ANDRI VAN MENS holds a Bachelor's degree in Political Science from the University of Montreal and is presently completing a Master's degree in International Relations at the University of Amsterdam. E-mail: asvmens@hotmail.com.

The authors wrote this article as interns at the Ministry of Defence of the Republic of Bulgaria during which time they helped organize an international seminar on *Promotion of Transparency and Democratic Decision Making in the Formation of SEE States Military Budgets* in Sofia (Bulgaria) on 6-7 June 2000. Their internship was organized by the Canadian-Bulgaria Business Council and financed through the Canadian Ministry of Human Resources Development Canada.

BACK TO TOP

Defence Budget Transparency on the Internet

Kate Starkey and Andri van Mens

Keywords: Defence resource management, confidence building, PPBS, budget transparency

Abstract: Fundamental to the security and stability of a region is communication and the sharing of information between neighbouring countries. This notion is especially true in the case of military budget transparency, where if states were to come to a common agreement on the sharing of defence expenditure information, confidence between neighbouring states would increase and the chances of military tensions would be reduced. This paper is a comparative study of what defence expenditure figures are available on the Internet for countries of the South European region as well as selected NATO and non-NATO member countries. In looking at how the topic at hand relates to issues of democracy, the study assesses what type of Internet-based information is available at the moment and how this information could be used to enhance regional military cooperation and understanding in South Eastern Europe. Although the Internet provides a constructive and clear framework for the purposes of the study, it also poses certain limitations. Taking into consideration these limitations, the article provides a firm basis for what more can be accomplished in the area of defence budget transparency with respect to the Internet.

Author: **Petar Mollov**
Title: **Participation in the Consortium of Defense Academies and Security Studies Institutes and Advanced Information Technologies**
Year of issuance: **2000**
Issue: **Information & Security. Volume 5, 2000**
Hard copy: **ISSN 1311-1493**

PARTICIPATION IN THE CONSORTIUM OF DEFENSE ACADEMIES AND SECURITY STUDIES INSTITUTES AND ADVANCED INFORMATION TECHNOLOGIES

Petar MOLLOV

Table Of Contents:

The participation of Rakovski Defense College in the activities of the Consortium of Defense Academies and Security Studies Institutes creates an opportunity for effective implementation of advanced information technologies in the educational and research activities of the College and promotes the reform in the military education system. It also contributes to the active participation of the Republic of Bulgaria in the "Partnership for Peace" (PfP) program and assists Bulgarian preparation for joining NATO. Knowledge of the purpose, aims, tasks and structure of the Consortium allows Rakovski Defense College, as well as other governmental and non-governmental, military and civil organizations and individuals, working in the sphere of security and defense, to take active and productive part in the process.

Background

The Partnership for Peace program was adopted at the summit of the North Atlantic Council in Brussels, Belgium, in January 1994 [1]. This program introduced new means for cooperation among

NATO members and partner countries. PfP aims at improving the peacekeeping capabilities of the participating countries by means of combined planning, education, training and increased interoperability of the armed forces. During the summit of the Euro-Atlantic Partnership Council of Defense Ministers on June12, 1998, the U.S. Secretary of Defense William Cohen presented new vision about the education and training in PfP. He suggested the establishment of:

- Consortium of Defense Academies and Security Studies Institutes;
- simulation network for exercises focused on peace support operation scenarios;
- cooperative network of nationally sponsored PfP training centers.

The First Annual Conference of the Consortium of Defense Academies and Security Studies Institutes took place in Zurich, Switzerland, in the period from 19 till 21 October 1998.

Consortium and Advanced Information Technologies

The Consortium is the major initiative of the Euro-Atlantic Partnership Council (EAPC) in the sphere of education and training in PfP [2]. Its main purpose is to improve the proficiency level in defense matters by expanding institutional cooperation in education and defense preparedness. It is envisaged that the utilization of advanced information technologies is a very important factor that affects network capabilities enhancement. The creation of a Consortium website was planned as an immediate task, followed by publication of an electronic magazine. The best chance of enhancing the efficiency of future work and saving resources in this area are provided by the agreement between Internet-based International Relations and Security Network (ISN) and US Defense Department's Partnership for Peace Information Management System (PIMS). Top priority is the development of Internet supporting instruments for civilian, governmental and non-governmental organizations, dealing with defense and security policy.

Participation in the Consortium is open for all organizations from the Euro-Atlantic Partnership Council member countries that agree to the adopted principles and desire to support or participate in it. [7]

Organization of the Consortium

The Consortium consists of members, Work Groups and Secretariat. Official languages of the Consortium are English, French, German and Russian. The main structural elements of the Consortium are:

Participant – a person, affiliate or supporter of the goals of the Consortium;

Member of the Consortium – a military/defense academy or a security studies institute from a country participating in EAPC, which supports the principles of the Consortium’s charter and has declared its desire to be a member of the Consortium;

Affiliate of the Consortium – an organization from a country participating in EAPC, other than military academy or security studies institute, which supports the principles of the Consortium's charter and has declared its wish to be Affiliate of the Consortium;

Supporter - an organization from a country participating in EAPC, which accepts the principles of the Consortium, but does not wish to be recorded as participant or adherent of the Consortium;

Secretariat – staff with international participation, which leads and coordinates the work of the Consortium;

Work group – a group of participants, members, adherents and supporters, who jointly work for the realization of tasks, projects or interests.

The supreme body of the Consortium is the Annual Conference.

The principles, declared by the participating countries, and functional-administrative activities of the Consortium are not officially committed documents.

IT-related working groups

The activities of some of the Working Groups are closely related to the advancement of Information Technologies to achieve the goals of the Consortium. Their mission can be summarized as follows:

Advanced Distributed Learning. To establish and maintain an open source, web based environment that links consortium member organizations in a collaborative network facilitating the development of Advanced Distributed Learning (ADL). To that end, plans and prototypes will be developed to include recommended architectures, functional requirements, technical standards, and other informational tools that will foster development and exchange of educational content by contributing members of the Consortium.

Archives Working Group. To help its members gain from training in modern archival working methods and to facilitate the exchange of experience. To serve as a clearinghouse for information on availability and accessibility of documents. To facilitate the preservation of and access to documents by providing the necessary technical assistance. To seek support for research, including identification, selection, and reproduction of the most important documentary sources. To promote public knowledge and understanding of past and current security issues by sponsoring translation and publication of selected documents, with analytical and interpretive commentaries, in both print version and online. To encourage the scholarly study of the military dimensions of the Cold war and its consequences for the current processes by organizing international conferences and workshops where new archival evidence is analyzed, interpreted, and presented for discussion.

Curricula. The work group on curriculum development seeks to contribute to the EAPC efforts towards creation of a cooperative network in security education by promoting excellence in curriculum development and course accreditation. For this purpose it will create, on a multilateral basis, a network dedicated to development, accreditation, validation and electronic distribution of

curricula in defense management and security policy. Trough its work and by assuring diverse views on curricula development and teaching, the group will foster civil-military relations, dialogue and understanding in the EAPC area. Given the current drive towards joint military and security policy education, the work group will attempt to create common EAPC standards for courses and other training activities.

Digital Library. The working group enhances cooperation in research and education through development of a comprehensive, international web-based digital library for political and military education.

Information Technology; Web Services. The workshop represents an ongoing effort to address all related concerns of participating institutions in the consortium. Emphasis should be laid on three primary pillars:

- Defining user requirements.
- Developing teaming relationships between organizations to address those requirements.
- Focusing on achievable, practical measures and short- to near-term projects.

The scope encompasses everything from organizations that can not even reach the web site (and so need either computers or communications means) to organizations that have large bodies of information (say their curricula) that need assistance in developing technical tools (databases, etc.) to help them manage and exchange the information.

Lessons Learned. The work group will focus on methodologies, technologies and content of lessons learned, and more generally, on what is needed to support an army, or other military or military-political institutions, as a learning organization.

Military History. Work group responsible for maintaining regular contact between official institutions and other scholars interested in cooperating on projects and sharing information related to military history.

Modeling and Simulation. This work group coordinates modeling and simulation, computer-aided exercises (CAX), and other simulation tools that facilitate training activities.

Publications. To provide a family of publications, covering the full range of security studies, to an international standard of excellence, serving military, civilian and academic needs of members of the Consortium.

Research. To link existing research sites, resources and personnel of consortium participants and to promote the establishment of common research projects in order to enhance security, defense, and military policy education and to facilitate knowledge and information sharing among EAPC nations.

Participation of "Rakovski" Defense College in the Consortium

The adoption of the National Security Concept in 1998 and the Military Doctrine in 1999 created conditions, for the first time since 1990, for a real and purposeful reform in the armed forces of the Republic of Bulgaria. A Plan for the organizational build-up of the Ministry of Defense by 2004 [3] was worked out on the grounds of these documents and the comprehensive study on the status of the Bulgarian Armed Forces, the prospects for world and regional development. [4,5] The above mentioned documents enabled the development and adoption of the *Concept for development of Rakovski Defense College, military academic education and scientific research*, as well as plan for its realization. [6] One of the basic functions, stipulated in the Concept, aims at introduction of modern technologies and training programs. The fulfillment of this function requires that the "G.S. Rakovski" Defense College perform the following tasks:

- To participate in the international academic cooperation aiming at developing interoperability in the military education, improving the forms and methods of education and expanding the modern military, technical and political knowledge.
- To take part in the international information exchange and represent Bulgaria in the Consortium of Defense Academies and Security Studies Institutes, i.e., in the area of security analysis.

The active role of Rakovski Defense College in the Consortium commenced after its Second Annual Conference. Under the leadership of the Deputy Commandant the Defense College, a brochure extensively covering the aims and basic principles of the Consortium's functioning was published. On 28th December 1999, the Defense College organized a meeting with the personnel, delivering information on the Consortium and providing the Defense College leadership with vision for the future development and required organization for effective participation in the Consortium. An Application Form for participation in the Consortium was offered. On 13th January 2000, the first association meeting of applicants from the Defense College took place. A Vision (presented in Appendix 1 to this article), general program and an academic organizational structure (Appendix 2) were adopted. In accordance with the program, the Commandant of the Defense College provided offices for the Consortium academic work groups. The Information Technology Work Group through its Co-Chair, PIMS Liaison to PfP Consortium, donated three computers, two printers, a web server and other hardware equipment.

This equipment has been of great use to the course participants and teaching staff in the Defense College. At that time, a great number of the computers that were in use in the Defense College were out-of-date and had no access to the Internet. The first Internet connection was established on 15th March 1999. Only the Interoperability Center and Education Department had Internet access. Most of the Defense College faculty members were not able to operate with advanced software products, e-mail or the Internet. This explained the eagerness of the participants in academic work teams to be involved in the work of the Consortium and in computer courses with respect to the above mentioned computer skills. With the assistance of the PIMS representative in Bulgaria all computers were connected to local and global networks by 14th January 2000. This enabled the continual access to the Internet. The equipment could be used 24 hours per day, seven days a week.

On 20th January 2000, Rakovski Defense College was registered in the Consortium website. Later on,

the registration of individual participants was carried out. On the grounds of the submitted application forms a data base was developed for the addresses, abilities and needs of the applicants taking part in the Consortium activities. 131 application forms have been submitted up to now. Contacts for cooperation on Consortium issues have been established with other governmental, non-governmental, civil and military organizations. Part of the academic participants are from the Bulgarian Academy of Sciences, General Staff, Bulgarian Armed Forces, History Association, National Sports Academy, etc. Several foreign representatives in the Consortium took part in two of the general meetings. These meetings were extremely beneficial for the Defense College activities and gave answers to a number of current issues concerning the Consortium's activities. The assistance of the British Council representative was also essential. Since the end of February 2000, the Deputy Commandant of the Defense College and Director of the National Security and Defense Department took over the management of the Consortium's activities. His participation in the Secretariat WG and his experience will play a crucial part in future activities. Defense College representatives took part in work meetings of the following groups: Military History (4-5 April 2000, Garmisch, Germany); Syllabus (14 April 2000, Geneva, Switzerland); Digital Library (18-21 September 2000, Garmisch, Germany); Advanced Distributed Learning (September 2000, Rome, Italy; January 2001, Geneva). Three officers from the Defense College took part in the Third Annual Conference of the Consortium, Tallin, Estonia (19-21 June 2000). Rakovski Defense College hosted the first session of the leadership of the "European Security and Defense Identity" work group (12-13 May 2000), as well as a work meeting of the developers of the Learning Management System project (4-8 September 2000). Representatives from eight countries participated. The Rakovski Defense College personnel were invited and given the opportunity to work in the group. Representatives from the General Staff of the Bulgarian armed forces, the Ministry of Transportation and private companies were also invited to participate.

The objectives of the workshop were as follows:

- To review the Program Management Plan.
- To review the development methodology to be used by developers across PfP organizations wishing to participate in this development project.
- To review the agreed upon schema for this phase of the development process, leading to a prototype that validates the users' requirements for subsequent development.
- To formulate questions to be answered by the development team, as well as requirements by eventual users of the system, that would affect development in the foreseeable future.
- To introduce new courses that validate our technical approach into new prototype database system.
- To provide a diagram of the system in its current state.
- To review procedures for setting up local copies of the entire distribution, working on a module, and submitting a module for consideration by the core technical lead team.

The Academic Curricula WG prepared an answer for the Curricula Questionnaire – Existing Courses and some of the syllabi of Rakovski Defense College, in relation with PfP, are included in the database of the Curriculum working group of the Consortium. Using the Consortium's equipment a

Website of the National Security and Defense Policy Department was created.

In September 2000, the Information Technology Working Group provided nine additional computers to the Rakovski Defense College and ensured their connection to the Internet. This contributes to the more efficient participation in specific projects. Furthermore, we intend to create a Website of the College and to take more active part in activities of Advanced Distributed Learning and Lessons Learned working groups.

In November 2000, the academic Lessons Learned WG representatives took part in the Workshop in the Center for Army Lessons Learned, Kansas, the United States. The group intends to create a national system to gather information for the Consortium PfP database. The participation in this initiative will ensure exchange of experience among partner countries gained during their participation in PfP exercises and operations.

In January 2001, at the ADL WG met in Geneva to discuss testing the Learning Management System at four sites. Rakovski Defense College is one of the places where the English Skills for Staff Officers course will be tested by instructors with the help of residential students.

An information bulletin about the activities of the Consortium and the participation of the Defense College was published, along with publications by authors from the College. We plan on participating in future work meetings, with an increased number of participants, in the separate projects of the Consortium. In this way, Rakovski Defense College contributes to the implementation of the Partnership for Peace Program.

Appendix 1

VISION

for participation of the "Rakovski" Defense College in the PfP Consortium of Defense Academies and Security Studies Institutes

In accordance with the newly developed PfP Training and Education Enhancement Program (TEEP) of the Euro Atlantic Partnership Council (EAPC) the Leadership of "Rakovski" Defense College intends to organize the implementation of the principles of the Consortium of Defense Academies and Security Studies Institutes within the College and to contribute to building regional and international security. To achieve these goals the following activities have been planned:

- To establish an appropriate organization;
- To register "Rakovski" Defense College for participation in the Consortium;
- To assist registration of individuals;

- To educate and train the participants;
- To provide necessary materials for participants;
- To establish preconditions for effective participation and contribution of the Defense College to various working groups' activities (without duplicating the Working Groups of the Consortium);
- To adapt the programs and teaching methods of the College to PfP Concepts and NATO standards;
- To participate in Annual Conferences of the Consortium and to actively promote new initiatives and specific suggestions;
- To prepare official statements of the Defense College about the participation in national and international activities within the framework of the Consortium;
- To extend contacts with other organizations;
- To maintain direct contact with the Secretariat of the Consortium of Defense Academies and Security Studies Institutions.

Appendix 2

ACADEMIC COORDINATION COUNCIL

The Academic coordination council does not duplicate the functions of the Secretariat of the Consortium of defense academies and security studies institutes. It does not restrict participants of academic working groups from direct contacts with the participants in international work groups of the Consortium. It directs the activities providing the necessary conditions for work in separate academic working groups that achieve the aims of the Consortium at the academic level.

To realize these functions, the following organizational structure is suggested:

- leadership;
- coordinators /co-coordinators/ of academic work groups.

Leadership includes a chairperson and a secretary. *The Chair* is a member of the College leadership - Commandant or Deputy Commandant of the College. He or she directs the overall activity of participation of the College in the Consortium. *The Secretary* is a member of the College staff. He or she organizes the activities of the Academic coordination council. The secretary is in direct contact with the coordinators of the academic work groups, summarizes the participants' requirement• and provides information and material support. He also manages the procurement cell.

Coordinators of the academic work groups are identified by the Leadership of the Academic

Coordination Council. They are specialists in specific areas and work on projects related to defense either in the College or other institutions. If the coordinator is a member of another institution, a co-coordinator is selected. The latter is a member of the College. The coordinators manage the participants' activities in the respective academic work groups. They develop a program for participation in certain activities of the international work groups of the Consortium.

Academic Work Groups. The academic work groups consist of participants, members, and supporters, who work together according to their interests, specific tasks and projects. They realize in practice the activities, planned in the general and individual programs. They have access to information and materials provided for the Consortium's activities. They are self-managed cells and define their own program, the structure for its realization, the time and place of their meetings. They are not limited in their contacts with the international work groups of the Consortium. The number and type of work groups corresponds to those accepted at the Annual Conference of the Consortium.

The academic working groups are supported by a "Supply Cell." It includes an assistant secretary, a system administrator and a person responsible for the materials. They are College members and are appointed by the Commandant.

Participant in an Academic Work Group is each person or supporter of the Consortium objectives, who has expressed his or her willingness to take active part in the Consortium activities.

References:

1. Lisa Bronson, *A Vision for the PfP Consortium* (1988).
2. *Concept for development of "Rakovski" Defense College, military academic education and scientific research* (Sofia, RDC, 2000).
3. Velizar Shalamanov, *The White Paper – Defining the vision for defense and the armed forces of Bulgaria for the XXI century*, http://www.md.government.bg/.
4. *Membership Action Plan* (Sofia, MoD, 1999).
5. *Plan for Organizational Development of the Ministry of Defense till 2004* (Sofia, MoD, 1999).
6. Victor E. Stamey, *The Way Ahead* (2000). This paper, as well as reports, conference announcements and further current information is available at http://pfpconsortium.org/
7. *The NATO Handbook*, 50th Anniversary Edition (Brussels: NATO Office of Information and Press, 1998).

PETAR MOLLOV is born in 1956. Colonel Mollov is pilot in the Bulgarian Air Force. He holds M.Sc. degree from "G. Benkovski" Airforce Academy (1979), Master degree (Operational art, 1989) and Ph.D. (Air Fire Deserting of Ground Targets, 1998) from "Rakovski" Defense College, Sofia (1989). Since 1999 he is associate Professor with over forty publications in the field of fight efficiency. Currently, Colonel Mollov is Chair in the Interoperability Department of "Rakovski" Defense College and Co-Chair of "Lessons Learned" Working Group of the Consortium of Defense Academies and Security Studies Institutes. Address for correspondence: Rakovski Defense College, 82 Evlogi Georgiv str., 1504 Sofia, Bulgaria. E-mail: mollovp@yahoo.com.

BACK TO TOP

Information & Security. An International Journal
e-mail: infosec@mbox.digsys.bg

Participation in the Consortium of Defense Academies and Security Studies Institutes and Advanced Information Technologies

Petar Mollov

Keywords: Partnership for Peace, PfP Consortium, Advanced Information Technology, military education.

Abstract: The participation in the Consortium of Defense Academies and Security Studies Institutes creates an opportunity for more effective implementation of advanced information technologies in educational and research processes. Knowledge of the purpose, the goals and the organization of the Consortium allows governmental and non-governmental, military and civil organizations, and individuals, working in the sphere of security and defense, to take active and productive part in the "Partnership for Peace" initiative. This article presents the experience of "Rakovski" Defense College, Sofia, Bulgaria, as member of the Consortium.

THE INFORMATION REVOLUTION AND POST-MODERN WARFARE

Steven Metz, *Armed Conflict in the 21st Century: The Information Revolution and Post-Modern Warfare* (Carlisle, Barracks, PA: Strategic Studies Institute, USAWC, April 2000). Available online at http://carlisle-www.army.mil/usassi/ssipubs/pubs2000/conflict/conflict.pdf

It is widely accepted that the advancement of communications and information technologies and their implementation by the military changes the nature of warfare. The consistent development of capabilities to find your enemy faster than he finds you, to decide quickly on a course of action, to precisely hit the enemy while limiting collateral damage, and to assess the results of your action, brings a new quality to warfare. Therefore, when expansive introduction of IT is combined with adequate organizational adaptation and doctrinal changes, students of warfare usually speak about "revolution in military affairs."

In his monograph Dr. Metz expands the treatment of ‘speed’ and ‘precision’. He examines strategic speed as equally important to success as the IT-based tactical and operational speed. Strategic speed requires not only mobility and readiness of the military, but also faster political decision-making. Readiness, mobility, airlift and sealift capabilities do not substitute for time consumed by consensus building. Regarding precision, thinking on the revolution in military affairs has so far addressed mostly its physical aspect, i.e., the ability to hit a target with great accuracy from a safe distance and to achieve precisely the desired physical effect. What is more important for the military strategist and commander, however, is to think in terms of psychological precision – to aim at attaining desired attitudes, beliefs, and perceptions both of enemy and observers.

On strategic level, this study of the effects of information revolution is not limited to technological transformation, computer viruses, attacks on commercial communications infrastructure and other potential manifestations of strategic information warfare. Rather, the author studies more broadly the strategic significance of the information revolution in terms of probable ‘combatants,’ available means and responses, and measures of success. Dr. Metz defines three types of war – ‘formal,’ ‘informal,’ and ‘gray area’ war, and focuses the reader’s attention on the complexity of the concept of *asymmetry* in future warfare.

The author admits that for the near future the US military may be the only state actor in post-modern warfare. Nevertheless, it may need to reassess basic defense planning assumptions. Particularly, regarding gray area wars, the creation of American national *gendarmerie* may be justified. In alliance with similar security forces of other states, it would operate more effectively against gray area enemies in an interconnected security environment and global economy. Likewise, nations may be better prepared for post-modern warfare even without sustaining large, peacetime military. Corporate armies and intelligence services may fill in the ranks in times of need. The military thinkers, however, should address in advance related new realms of strategy, policy and legitimacy.

Several other ideas in this monograph pose intellectual challenges to force planners. For example, Dr. Metz suggests that current division of the military in army, navy, and air force may not be adequate a few decades from now. More appropriate may be to organize the military along types of conflict.

Another example relates to the flattening of organizational structures, characteristic for effective information age businesses. Accordingly, it is proposed that we reconsider the separation between officers and enlisted personnel.

A common theme throughout the book is change management. To sustain effective military in the information age, the leadership of the armed forces should have the intellectual, psychological, and organizational capacity and the will to anticipate, plan and implement change; on a permanent basis. An alternative driver for change would be battlefield defeat. With this thought provoking book Steven Metz argues that it is possible visionary leadership rather than blood to inspire necessary changes.

Todor Tagarev

NEW AFCEA CHAPTER IN SOUTH-EAST EUROPE

On May 12, 2000, in Varna on the Bulgarian Black Sea coast new Chapter of the Armed Forces Communications and Electronics Association (AFCEA) was founded. This second Bulgarian Chapter of AFCEA will pursue the objectives and abide to the principles of AFCEA International paying special attention to the Navy and marine technologies and, thus, contributing to the success of the Bulgarian military reform, as well as to strengthening the maritime power and national security.

Chapter "Varna" will try to spread its activities to the whole Bulgarian Black Sea coastal area and, in mutually supporting and complementing cooperation with Bulgarian Chapter "Sofia", to contribute to the wider dissemination of the ideas and activities of AFCEA throughout Bulgaria, South-East Europe and the Black Sea region, thus contributing to regional stability and peace.

The founding meeting elected in the Chapter's Board active and retired naval officers from the Bulgarian Navy HQ, from the Naval Academy and research institute, as well as representatives of the high-tech business community.

At the time of its formation, Chapter "Varna" had 28 individual chapter members and two corporate sponsors (Unimasters Logistics Group Ltd., Varna, and the Institute of Air Transport, Sofia). By the end of 2000, Chapter "Varna" had 34 individual members (among them the US Defense and Air Attaché in Sofia) and one more corporate sponsor (WESTEL Ltd., Sofia).

During the few months since its establishment, the AFCEA "Varna" Chapter proved its value as a center for defense and security related knowledge sharing, business contacts and personal development. It regularly holds meetings, lectures and discussions. Of particular interest to AFCEA members was the visit on board USS Hawes (FFG 53) allowing first-hand familiarity with the C4I systems and capabilities of the ship.

For less than six months AFCEA-Varna Chapter hosted the following speakers:

- Dr. Velizar Shalamanov, Deputy Minister of Defense for Defense Policy and Planning, "The Introduction of Contemporary C4I Systems in Bulgarian Armed Forces as a Vital Element of Bulgarian Defense Reform."
- Brian Shade, Partnership Marketing, Denver CO, "Use of Data in Contemporary Economy."
- Captain (BuN) Tchavdar Ormanov, "Combat Information Systems in Bulgarian Navy."
- Eberhard A. Mueller-von der Bank, Regional Vice President, AFCEA Central European Region, "Objectives, Organization and Functioning of AFCEA in Europe and in the Central European Region. The Role of AFCEA in the New Security Environment."
- Captain (BuN) Nikola Kolev, Varna Naval Base, "The 'EKRAN' Project: Current Status and Future Prospects."
- Colonel Roger Fielding, UK Defence Attaché in Sofia, "The UK and the New NATO."

- Prof. Boyan Mednikarov, Naval Academy, Varna, "Improving the Combat-and-Information Capabilities of Bulgarian Navy Strike Forces."

AFCEA Chapter "Varna" address:

40, Graf Ignatiev Street
P.O. Box 229,
BG-9000, Varna, Bulgaria
Phone: (00359 52) 6655 777; Fax: (00359 52) 6655 755
Internet web site: www.afcea.bg
E-mail address: secretary@afcea.bg

Peter Strantchevski

INFORMATION ASSURANCE CHALLENGES

A two-day seminar on *Information Assurance* was held in December 2000 in the "Ribaritza" Hotel located in the picturesque resort with the same name in North-Central Balkan mountains. The seminar was organized by the Defense Planning Directorate, in cooperation with the Institute for Advanced Defense Research, in fulfillment of decisions taken during the interagency meeting held in November 2000 at the "G. S. Rakovski" Defense College in Sofia. Its main objectives were to provide information on advanced commercially available technological solutions and to facilitate discussion among specialists working in various fields related to information assurance.

The program of the seminar included presentations of corporate solutions in the area of information security as follows:

1. Corporate policy for information assurance – Microsoft, IBM, Hewlett Packard, Oracle;
2. Comprehensive security solutions – Cisco Systems, ACT Sofia, Computer Associates, LIREX BG, S&T;
3. Solutions for communications security – CRYPTO AG;
4. Anti-virus protection and support – Infoguard, National Laboratory of Computer Virology;
5. Specific technological solutions for information security – Electron Progress, BETA.

The seminar was attended by representatives of the Ministry of Defense (Defense Planning Directorate, Institute for Advanced Defense Research, Military Information Service, Legislative Directorate, J6, Military Counterintelligence, Administrative and Information Support Directorate), Ministry of Interior (Communications Protection Service, Institute for Computer Technologies, National Security Service), Ministry of Transportation and Communications, the National Laboratory of Computer Virology at the Bulgarian Academy of Sciences, scientists from the Sofia University.

The participants discussed a draft "Concept for assuring information for security and defense," as well as legislative, organizational and technological issues related to information protection requirements for NATO integration.

Svetoslav Shumanov