Information & Security Volume 6, 2001

C4ISR in Force Modernization

Edited by Velizar Shalamanov and Todor Tagarev

IT in support of Defense Reform

I&S Monitor

C4 Initiatives

I&S Research Centers

Author: **Editorial**
Title: **C4ISR for Advanced Defense Capabilities and Security**
Year of issuance: **2001**
Issue: **Information & Security. Volume 6, 2001, pages 5-6**
Hard copy: **ISSN 1311-1493**

C4ISR FOR ADVANCED DEFENSE CAPABILITIES AND SECURITY

For more than a decade we accept as ground truth the thesis that advanced communications and information technologies, if wisely implemented, are a force multiplier. They allow the warrior to see better, to have a better orientation, to make adequate decisions faster, to hit more precisely, to access the decisions of his action more accurately. With the unfolding of the information revolution and the end of the Cold war, the information technology may become more than a force multiplier and to turn into a vehicle for promotion of regional and sub-regional security arrangements. This is particularly true after the terrorist attacks on September 11th, with the understanding of the need for comprehensive interagency and international cooperation.

No single agency may deal effectively with the new security challenges. Practically, not even single country or international organization can do that. A complex threat needs a complex response. Political, diplomatic, economic and financial, law enforcement, military and informational means of a number of actors have to be integrated in a seamless manner.

This is not a simple task even under normal circumstances. But when you search for solutions under severe resource constraints, lack of market experience and a variety of cultures of former enemies, the challenge is worth even for the most adventurous. Nevertheless, we believe that it is possible to find solutions through evolutionary development of cooperative crisis management capabilities – capabilities to collect and share information, capabilities for cooperative decision making, capabilities to control cooperative response, and capabilities to train and learn together.

This issue of *Information & Security* looks for ideas how to implement advanced command and control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) technologies and systems to build and sustain cooperative crisis management capabilities in the region of South East Europe. The articles are based mostly on the experience of Bulgaria in developing defense capabilities through advanced C4ISR. However, they provide a glimpse at the potential of C4ISR in interagency cooperation and cooperation among the countries in the region.

Of particular importance is the approach to the acquisition of C4ISR systems when there is no obvious leader in the region, budgets are limited, technologies come from outside, and the pace of their development often exceeds the pace of political and expert coordination. In transition periods, it is a challenge to provide effectiveness of defense acquisition even for a single country. Joint procurement is not easy for countries that have been cooperating politically and economically for decades. Nevertheless, we believe that there is a great potential for joint procurement initiatives in South East Europe, and to start with procurement of C4ISR systems is the obvious choice.

The political framework is there. The United Nations and OSCE support regional security arrangements. The willingness of Western Europe and North America to sponsor the process, mostly through the Stability Pact for South East Europe, is proven. Success of SEE Defense Ministerial Process (SEDM) in the framework of Partnership for Peace/EuroAtlantic Partnership Council is great contribution to the regional security and stability. The countries in the region have the talent in labor, research, education, etc. The attraction for the business is there with the emergent market for C4ISR systems, and for advanced information and communications technologies in general.

If this volume of *Information & Security* provides even tiniest acceleration to the process of regional security cooperation, it will meet our bravest expectations.

BACK TO TOP

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

Author: **Velizar Shalamanov**
Title: **C4ISR in Modernizing Security Sector in Bulgaria and South-Eastern Europe**
Year of issuance: **2001**
Issue: **Information & Security. Volume 6, 2001, pages 7-22**
Hard copy: **ISSN 1311-1493**

C4ISR IN MODERNIZING SECURITY SECTOR IN BULGARIA AND SOUTH-EASTERN EUROPE

Velizar SHALAMANOV

Table Of Contents:

Introduction

In the 1994-1998 time period, the mismatch between the requirements of the new security environment and the organization of the defense and security sector in Bulgaria reached its peak. In a declining economy, the country largely kept the force structures inherited from the Cold war. The discrepancy between ends and means, organizations and resources became particularly visible after February 1997 when the Interim Government of Bulgaria declared the will of the country to join NATO.[1]

The reform of the security and defense sector is based on sound and comprehensive political process. The National Assembly (the Bulgarian Parliament) approved new National Security Concept [2] and Military Doctrine.[3] In the implementation of the Parliamentarian decisions, the Government authorized a set of defense reform plans [4] and Plan for preparation for NATO accession [5] that later became known as the Bulgarian Membership Action Plan (MAP).

All national security and defense planning documents acknowledged the importance of advanced communications and information technologies. Furthermore, the Military Doctrine of the Republic of

Bulgaria declared that priority in the modernization should be given to command and control, communications and information systems, intelligence, navigation and surveillance systems.[6]

Significant progress was made in the last three years in Bulgaria in implementing the decisions for priority development of the C4ISR [7] systems. The thesis in this article is that reform is needed to modernize C4ISR systems but, on the other side, the modernization of C4ISR may be important driver for force modernization, organizational change and the adoption of new service culture. Of particular importance is the potential of advanced C4ISR systems in enhancing security cooperation and the build-up of cooperative crisis management capabilities in South-Eastern Europe (SEE).

In this article we examine several aspects of the role of C4ISR as force and reform multiplier. First, we analyze the link between C4ISR projects and overall modernization effort. Secondly, the review of different C4ISR projects is given in order to define environment for their implementation. Third, elements of life cycle support and international cooperation issues are discussed in order to present a comprehensive strategy for C4ISR program development.

Force Modernization and C4ISR

After the most difficult political decision were made, the next single most important factor for security and defense reform is *modernization* of the armed forces and security sector as a whole. In this effort, C4ISR projects will be of crucial importance. Their implementation will impact multidimensional:

- A number of important and expensive project have been already launched;
- There are many positive developments in the normative and expert environment;
- Their implementation will lead reform processes in other areas;
- C4ISR will provide interoperability, security and will integrate everything else around them in one security and defense system of new type, that can be considered as *e-Security & Defense* part of the e-Government.

Modernization as a whole includes *utilization* of the surplus of obsolete or equipment that is difficult to support, not interoperable, or simply not adequate to the requirements of the Military Doctrine. Second component is *modernization* of the equipment that can serve next five-ten years. Third component is the *acquisition* of the new, probably in some cases second hand, equipment that will serve at least in the next twenty years.

Of particular importance is to harmonize modernization plans with risks and threats, complete set of missions, structure of the armed and security sector forces, system of training and life cycle support capabilities of the country and, last but not least, available resources, R&D and industrial capacity.

Additionally, IT can dramatically to improve quality of implementation of the modernization plan through the system of program management and overall life cycle management. [8] It allows to involve in modernization planning the administrative organization of security & defense forces, industry, the academic sector, non-governmental organizations (NGOs) and the broader civil society.

C4ISR systems are specific, because they are based on the most rapidly changing technologies. Interoperability and dual use issues are of critical importance for them and life cycle is based more on evolutionary prototyping and development than on “under key” approach of developing systems, that can be operated next several years without significant upgrade and improvement. [9] These systems are very sensitive from the security point of view because, first of all, they keep all the information and, secondly, they control all other systems.

Furthermore, C4ISR systems and related projects have a crucial role because they integrate existing platforms in combat complexes, provide interoperability in the key C2 areas dealing with the most important resources - information and knowledge. At the same time, just these systems are becoming obsolete most rapidly and, as was mentioned above, that impacts information security that is critical under rapid technological changes and convergence with civil systems.

Finally, C4ISR systems are unique because of the integrating role they play in combat complexes and the procedures for life cycle support. In the context of process of rethinking underway, and the changes after the tragedy of September 11th, 2001, it is clear that C4ISR systems will be even more important for and at the same time will be strongly influenced by the coming strategic shift.

While debating modernization issues, the following aspects of the role of C4ISR projects have to be covered:

- Classification of C4ISR systems and projects;
- Life cycle management of C4ISR systems;
- Business aspects of C4ISR system development, especially integration and cooperation among companies, both suppliers and system integrators.

Classification of C4ISR projects

There are several aspects of classification of the C4 projects, but for purposes of our analysis the following criteria for assessment of the systems will be used : [10]

1. National / International (combined for many nations)

2. Type of C2:

    - military;
    - civilian;
    - mixed (dual use military with civilians);

3. Level of C2:

- strategic;
- operational;
- tactical;

4. Service/Institution/State of support

- Joint for all services:
    - Personnel;
    - Intelligence;
    - General / Operations, including special operations;
    - Logistics;
    - Long-term planning;
    - Communications & Information Systems;
    - Training;
- Army;
- Air Force;
- Navy;

5. Content:

- pure C4ISR;
- mixed: linked with platforms;

6. Mobility

- fixed;
- field;
- mobile;

7. Period of use:

- peacetime;
- time of emergency/crisis and transition periods;
- wartime.

In 1999, Bulgaria jointly with a team of US experts conducted a comprehensive C4 Study. [11] It followed a conference in which twelve countries participated. [12] The goal of the study was to identify key requirements for interoperability for all type of systems, priorities in their development, architecture and organizational issues of their life cycle management.

The study facilitated not only planning of C4ISR systems development, but also procedural and organizational adaptation. In combination with the introduction of the defense planning, programming and budgeting system, it provided for effective use of 50-70 mln. Levs [13] from the Bulgarian state budget per year and additional 20 mln. Levs in average from foreign assistance programs for investments in the building of modern C4ISR systems. So far, the Ministry of Defense is the main beneficiary of security assistance programs. However, security investments would be much more effective when C4ISR system development is consolidated for all elements of the security sector: Ministry of Defense (MoD), Ministry of Interior (MoI), Ministry of Foreign Affairs (MFA), the Civil Protection Agency and others.

The main C4ISR projects currently underway are:

1. National Military Command Center (NMCC) - strategic level project, integrating all lower level systems not only from MoD, but also MoI, Civil Protection and other security sector elements;
2. Automated Information System (AIS) with a number of subsystems;
3. Fixed Communications System (FCS) as backbone for AIS;
4. Field Integrated Communication and Information System (FICIS) - mostly for the Army, but related to C2 systems of the Air Force and the Navy. It has components at the following levels:
    - operational level for Rapid Reaction Forces (RRF) from Army, Air Force, Navy and Special Operations forces;
    - tactical level – national and regional, including the C2 system of the South-East European Brigade (SEEBRIG);
5. Air Sovereignty Operation Center (ASOC), including Command Posts, radar network (fixed and mobile), communications system (fixed and mobile), system for identification “Friend or Foe,” including onboard equipment for platforms;
6. Navigation and communications equipment for the airfields (NAVAIDS), including onboard equipment and C2 elements of the Air Force;
7. Sea Surveillance system “EKRAN,” related to the development of the vessels traffic management and information system (VTMIS). It includes onboard equipment and C2 for the Navy.

Additionally, the development of Computer Assisted Exercise (CAX) systems is essential. Another essential aspect is security--not only information security and information assurance, but also physical security of C4ISR facilities, personnel security, technology and industrial security, document security,

etc. Signal Intelligence, or even the broader spectrum of technical intelligence, issues are urgent as well. Similar systems for Civil Protection, Ministry of Interior and Complex Automated C2 System of the State are ongoing or forthcoming. Interagency and international cooperation and integration are crucial for the effective implementation of C4ISR technologies.

Most of the above projects are implemented using FMF [14] sources or money from the defense budget. However, additional effort is needed for integration and overall architecture design. [15] These projects cover all type of systems listed in the proposed classification. Initially, their implementation creates islands. When a common architecture is used, these islands can be easily and effectively integrated. Thus, in three to five years the Bulgarian armed forces will have a totally new C4ISR system that can be easily integrated for the national security sector. Furthermore, it can be integrated regionally in the framework of SEDM (SEE Defense Ministerial Process) and Stability Pact Working Table #3, as well as with NATO and the European Union. We strongly believe that is the wining strategy both on national and on regional levels.

Projects can be divided also on current (ongoing) and future ones. In any case integration at all levels is essential, and not only technically. In this respect long-term business strategy taking in account the long-term reform and modernization strategy of Bulgaria, NATO, EU and western companies is essential. Classification of systems is a way to assess how to position different companies, both foreign and from the Bulgarian defense sector, and how to build a consortium of all interested in building and supporting the emerging national and regional C4ISR system.

For some of the projects there is need for sizable Research and Development (R&D) and Education and Training (E&T). It is more effective to provide R&D and E&T support in Bulgaria on the basis of existing arrangements in the “Rakovsky” Defense and Staff College - centers of excellence, Interoperability Faculty, Institute for Advanced Defense Research with Research, Demonstration and Certification Center, Cisco and Microsoft Academies. Significant is the potential of the Bulgarian Academy of Science (BAS), which under the framework agreement with the Ministry of Defense recently established Center for National Security and Defense Research.[16]

The implementation of C4ISR projects can be supported also by establishment, locally, of:

- Software development center /Center for evolutionary software development;
- Software support center;
- Research, demonstration and certification center;
- Complex test-bed.

The Bulgarian experience shows that it is more effective to establish this type of support outside the Ministry of Defense. We believe that this practice may be facilitated if cooperation between different C4ISR contractors is established. Finally, this is an opportunity for direct and indirect offset programs that has been underutilized.

The Center for National Security and Defense Research in BAS can play a great role in that respect.

There is a formal link between the Academy of Sciences and the Ministry of Defense through the framework agreement. BAS research units and scientists, under coordination of the Center, participate in the Dutch- Bulgarian cooperation in defense research and technology. Forthcoming Memorandum of Understanding between UK and Bulgaria in respect of defense materiel cooperation will provide additional opportunities for ministry-to-ministry and company-to-company relations, where defense and dual-use research and technology and training support will be of significant importance.

Finally, for most of these projects joint efforts on regional basis will be essential. Naturally, many of the projects involve cross border systems, require exchange of data and information and work as part of even larger "network of networks." This is the reason to carry on with the experience from the first regional C4 Conference (June 1999) and to proceed with the establishment of C4ISR Coordination Group at least in SEE Defense Ministerial Meetings (SEDM) format. Thus, certain distribution of labor and regional approach to software development, support, maintenance, tests, etc., can be pursued. Again, this requires cooperation with main contractors for C4ISR projects in the region.

A successful example of such cooperation in South East Europe can be extended towards the Caucasus / Black Sea region, Central Asia, and the Mediterranean. The area of C4ISR is a good starting point to address other security and defense modernization issues and to build the basis for future joint procurement projects, i.e., projects involving acquisition of new platforms.

C4ISR as element of security sector modernization and life cycle management

Currently, the Bulgarian Ministry of Defense jointly with an US contractor conducts a comprehensive force modernization study (FMS). [17] The results of the study will be consulted with NATO through the Defense Support Division of the Alliance and will serve as basis for development of long-term plan for modernization of the Bulgarian armed forces. Ideally, the plan will provide for coordinated development of platforms, defense industry and the academic sector. In long-term the plan shall outline the development of airplanes, surface to air missile squadrons, ships, main battle tank modernization, armored personnel carrier modernization, artillery, including modernization of anti-tank weapons.

Another aspect is planning of the utilization of the large inventory of platforms, small arms and light weapons, ammunitions. Platforms will be assessed in context of the doctrines and emerging C4ISR systems, which are far ahead in modernization than any other element of the military complex. Main criterion should be how efficient they will be to exploit comparative advantages of Bulgaria. Logically, the companies involved in C4ISR projects that have capabilities also in the area of platforms can be a factor for integration in the overall modernization effort. On the Bulgarian side such factor potentially is the company TEREM because of the scope of its competencies and experience in dealing with MoD and other elements of the security establishment. On the other hand TEREM is still state owned, so it may potentially serve as a kernel for building "National Defense Industry Consortium" - a private company (SHC), that can be flexible in international cooperation and, eventually, allowing for foreign investments trough privatization.

There are seven important steps in a force modernization study:

- preparation (identification);
- fact finding and processing in different groups (differentiation);
- analysis, definition of recommendations (integration);
- development of modernization plan;
- gaining public and business support for the modernization plan;
- approval of the modernization plan by the Government and the Parliament;
- implementation through network of organizations for life cycle support of different types of systems.

The study covers nine different areas of modernization, respectively modernization of weapon systems and equipment of Army, AF, Navy, Logistics, C4, ISR, Defense and dual use infrastructure, Utilization, Defense industry.

Integration of the platforms through C4 is essential. At the same time, C4 infrastructure needs its own integration through a control center (Network Control Center - NCC). The development of NCC is part of the implementation of C4 projects. Integration is only one of the requirements. Rather more difficult is to achieve interoperability with NATO, flexibility, security, readiness, etc.

Finally, the C4ISR system is planned on at lest three levels: as set of equipment with certain capabilities and fixed structure; as task/operation oriented temporary and mostly mobile structure; and as real time response for immediate event driven reconfiguration. Normally, this planning is directly related to operational planning and planning of the use of platforms that will be controlled trough the C4ISR system. [18] That turns *the environment for configuration planning and management* into an essential factor for the success of any C4ISR system.

Organizational issues

In order to address more efficiently the issues of C4ISR life cycle management, the Bulgarian Ministry of Defense established the institution of Chief Information Officer (CIO). Further, it introduced *Manual for life cycle management* that clarifies organizational structures and procedures to maintain such a system from the idea about the system to its disposal and utilization. From national point of view, after regulation of the issue inside MoD, it is important to extend these efforts outside MoD and to prepare national level environment for management of the life cycle of C4ISR systems. That would include introduction of CIOs institutions, Program Office for C4ISR, and designated operators of the C4ISR in other governmental agencies.

On the other side, there is need for cooperation among the companies that are already involved in modernizing the C4ISR system. Thus, American and European companies may coordinate their efforts and to cooperate more closely with the Bulgarian defense and civil industries, for example in offset programs, E&T, R&D, testbeds (research, demonstration and certification centers), etc. TEREM can cover all type of platforms and some kind of C4ISR equipment, but there are many others that can join the club. As discussed previously, the “club” has to be around a private company

with participation of MoD and the Bulgarian Academy of Sciences.

Such organization would provide for cooperation on many levels:

- overall management of the process and alliance to modernize defense and security establishment;
- command and control centers (incl. NCC);
- C4ISR architecture;
- platforms.

The issue of defense industry involvement is closely related with the restructuring and strategic plan for the development of this sector. A recent study by the US Atlantic Council working group was a positive first step [19]; it has to be deepened and converted into full scale strategy and implementation plan.

When such environment is established, projects can be divided among the companies trough partnership agreements, still allowing for transparent competition and cooperation.

Non-governmental organizations (NGOs) can also be instrumental in providing transparency and coordination. Among many NGOs that are potential participants in such arrangement, we would refer to the “George C. Marshall” Association, covering broadly the security area from security policy to security sector reform and then to acquisition and defense industry restructuring. Given improved coordination, the activity of AFCEA (Armed Forces Communications and Electronics Association) in Bulgaria can give a substantial boost to interagency and international coordination. Another opportunity is the establishment in Bulgaria of an organization similar to the US “Business Executives for National Security” (BENS).

The potential for regional cooperation has not been utilized. The regional security cooperation in South East Europe, involving Albania, Bulgaria, Croatia, Macedonia, Slovenia, Romania, Greece, Turkey, Italy and, hopefully soon, Yugoslavia, Bosnia & Herzegovina has significant potential. Then it would be possible to create a network of networks in which the region of SEE cooperates with Central Europe, the Baltics, the Caucasus, Central Asia, and the Mediterranean region.

The SEE Defense Ministerial (SEDM) process provides a feasible framework for cooperation and *joint procurement, joint training and certification*. A priority area for joint procurement will be C4ISR. With this in mind, SEDM countries initiated the establishment of Regional Coordination Group (Committee). We envision further progress with US support; one opportunity for discussions will be provided with the Second regional C4 Conference in May 2002 during HEMUS 2002 Defense Exhibition. The main topic of the conference will be life cycle support of C4ISR systems on national, regional and interregional basis. We expect participation of major American and European C4ISR contractors.

Strategy in C4ISR area

There is a need to define large project for national C4ISR system to cover all aspects of National Security information requirements. [20] This can be a step to *e-Government Program*. From Bulgarian side such an initiative can be successful, because of:

- future membership in NATO and EU;
- Non-permanent membership in the UN Security Council and forthcoming chairmanship of OSCE;
- geo-strategic position in SEE, Black Sea region and leading role in many regional initiatives;
- good crisis management and emergency management experience and institutional cooperation;
- good progress in defense / security sector reform;
- advanced arrangements in C4ISR area, including legislative and organizational arrangements and, most importantly, trained and motivated people;
- existing set of projects in critical C4ISR areas funded through FMF and national funds;

It is important to address large program in order to resolve existing conflicts around small short-term bids and to open space for long-term strategic cooperation among major American and European defense companies and the Bulgarian defense industry. Small projects normally generate problems, often because of lack of vision, interoperability and efficiency issues, insufficient involvement of top-level management, corruption of low level-management, lack of interest for long-term strategic partnership with Bulgarian companies.

The National C4ISR System is good option, because it covers all elements of the National Security System, starting from the President:

1. Strategic Network with integrated National Command Center (Fixed, Stationary);
    - National Command Authorities (President with Consultative Council on National Security, including National Intelligence Service and National Service for Protection; Prime Minister with the Security Council; Supreme Command and why not Parliament with its Commission on Foreign Policy, Security and Defense as an element of decision making even on operational level (Such opportunity is envisioned in Article 84 of the Constitution);
    - Ministry of Foreign Affairs, including embassies around the world;
    - Ministry of Defense, including the General Staff and Special Commands;
    - Army;
    - Air Force and Air Defense;
    - Navy;
    - Ministry of Interior;

- Ministry of Justice;
- National Police;
- Gandarmerie;
- Border Police;
- Fire Brigades;
- Organized Crime Fighting Service (OCFS);
- National Security Service (NSS);
- National Investigation Service (NIS);
- State Agency for Civil Protection;
- Ministry of Transportation and Telecommunications, Ministry of Regional Development and Construction, Ministry of Healthcare, Ministry of Finance, Ministry of Ecology, etc.

2. Operational Level / Theater Level Command Post (Mobile, Field) integrating all tactical level information in common operational picture for C2 support and reporting to the strategic level command posts.
3. Tactical level Command posts of:

    - Army brigades;
    - Airforce bases / aircraft;
    - SAM squadrons;
    - Radar positions;
    - Navy bases, ships;
    - Ministry of Interior Teams (with regional team center);
    - National Police teams, including teams from NSS, OCFS, and NIS;
    - Border Police Teams
    - Gandarmerie teams;
    - Fire Brigade teams;
    - Civil Protection teams (with regional team center);
    - other ministries teams (with regional team center).

National C4ISR is to integrate in Information Grid following sub-grids:

1. Sensor Grid (radar, SigInt and other elements);
2. Navigation Grid;
3. Identification Grid;
4. Communication Grid;
5. Platform Grid;
6. Kernel - C2 Software Grid to support decision making;
7. Information Assurance Grid.

Overall concept is to have C2 software Grid supporting Common Operating Environment based on web (Internet) software. That means to have IP/VPN Communication Grid leading to Sensor, Navigation, Identification and Platform Grids that can generate/use data from web-based environment. Finally, the Information Assurance Grid has to be oriented to secure IP/VPN and web environment. So *technical proposals for all the grids have to be developed and integrated on the basis of IP/VPN communication grid and web-based C2 software*.

It is clear that, initially, IP/VPN capabilities will be down to certain level, for example highest tactical (brigade, base, regiment, regional team center). At the same time, there will be narrow band back up for voice and low-rate data communications, as well as other emergency reserve networks with narrow-band radio.

Most of the fixed infrastructure can be leased (outsourced), but field / mobile IP/VPN and narrow-band back-up communications is operated by government unit (common for all the elements of National Security System).

In this case there are certain organizational consequences for the Information Grid (IG):

1. IG High Level Management (HLM) - CIO and Program Office;
2. IG development & integration alliance (DIA);
3. IG Operator;
4. IG outsourcing contractors;
5. IG maintenance centers;
6. IG research and development / education and training centers;
7. IG C2 software development center.

Most critical is the question of high-level management and DIA – Development and Integration Alliance. The former is a governmental body, while the latter is alliance among mostly private companies to prepare together System Project and to build together all elements of the Grid. Definition and certain steps have to be taken to strengthen existing organizational elements and to

build some new, as well as to document activity of these entities according to the technical requirements of the information network.

Probably certain legislative amendments will be needed to establish best environment for operation of the above mentioned organizational entities (some of them formed of foreign companies), because functions like telecommunications and defense acquisition are too sensitive, especially in transition period.

A possible strategy should include the following steps:

1. Review of the FICIS project and definition of strategic partner for extension of the FICIS project to cover other elements of the force structure by Bulgarian IG – Bulgarian Security and Defense Information Network (BSDIN);
2. Review of the ASOC Project and definition of strategic partner for extension of the project, as well as to implement similar approach for the VTMIS project, both of them as part of BSDIN;

Above steps will provide:

- involvement with Army, AF and Navy;
- definition of areas of competence and cooperation with strategic partners.

3. Definition of proposals to Ministry of Interior, Ministry of Justice, Ministry of Foreign Affairs and State Agency for Civil Protection to cover their CIS requirements;
4. Participation of formation of Alliance of American and European C4ISR companies in Bulgaria and establishment of joint strategy for the next 10 years;
5. Involvement of key local defense industry companies to be part of the Alliance;
6. Engaging local R&D (mainly Bulgarian Academy of Science) and E&T (mainly Defense Staff College, Service Academies) in the Alliance.

It is clear that only good cooperation and harmonization of interests and capabilities can generate such a project. At the same time, this project is not starting in a void - there are many accomplishments in the area of C4ISR and a number of ongoing projects. Therefore, right now consolidation of all existing, ongoing and planned projects in large IG program is very important and will be good example for the even larger e-Government program. But to start with National Security System is essential especially because of the Bulgarian integration in NATO and EU, membership in the UN Security Council, future chairmanship of OSCE, and the growing demand for security cooperation after September 11th. The IG will integrate all elements of National Security system efficiently and will provide international integration, as well higher interoperability with NATO/EU countries.

Conclusion

The role of C4ISR projects is essential for overall modernization efforts, because of the influence on force structures and decision making processes. C4ISR developments impact security, interoperability, horizontal and vertical integration, cooperation with civil sector and the use of civil resources for security and defense. They are unique from technological point of view and influence of life cycle management.

On the side of the Government, certain arrangement were already made in the area of requirements definition, planning and programming, acquisition, R&D, E&T, testing and evaluation. Partnership among business companies and between business companies and Government is essential. There is an opportunity and a need for additional efforts in this area to provide better environment for successful implementation of C4ISR projects.

Notes:

1. Jeffrey Simon, “Bulgaria and NATO: 7 Lost Years,” *Strategic Forum*, Paper # 142 (Washington, INSS, National Defense University, May 1998).

2. National Security Concept of the Republic of Bulgaria, *State Gazette* 46 (22 April 1998). Available full text in English at http://www.md.government.bg.

3. *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.

4. Generally known as “Plan-2004.”

5. Velizar Shalamanov, “Priorities of Bulgarian Defense Policy and Planning”, *Security Policy* 2 (1999): 3-21.

6. *Military Doctrine,* Article 97.

7. Command, control, communications, computers, intelligence, reconnaissance and surveillance [systems].

8. Todor Tagarev, "Economic aspects of defense modernization," in *Economic Benefits for Bulgaria from Joining NATO* (Sofia: Centre for Liberal Strategies, 2001), pp. 25-42..

9. *C4I Study for Bulgaria: Final Report* (USAF ESC/MITRE, January 2000).

10. Velizar Shalamanov, *Information Environment for Analysis and Assessment of Military Threats* (Sofia: “Rakovsky” Defense and Staff College, 1995).

11. *C4I Study for Bulgaria*.

12. *C4/National Crisis Management Center Conference* (Sofia, Bulgaria, 21-23 June 1999).

13. Under the rules of so called “Currency Board,” the Bulgarian currency has a fixed exchange rate with the German Mark: 1 BN Lev = 1 DM.

14. The US program for Foreign Military Financing.

15. Good example in the respect is the project for operational, system and technical architecture design for the Army C4 system, started in the end of 1999 with BAE Systems as main contractor. We expect that the Ministry of Defense will provide conditions for the successful accomplishment of this project. The inclusion of the C4 systems of the Bulgarian Air Force and of the Navy is strongly recommended.

16. The Center is presented at the end of this volume.

17. For details see Todor Tagarev, “Prerequisites and Approaches to Force Modernization in a Transition Period,” in this volume.

18. Velizar Shalamanov, *Life Cycle Support of Information Systems Management*, Doctoral Dissertation (Kiev: Air Defense Radioelectronics Institute/Institute of Cybernetics, March 1991). in Russian

19. Curtis M. Coward and Jeffrey B. Bialos, *The Bulgarian Defense Industry: Strategic Options for Transformation, Reorientation and NATO Integration* (Washington: The Atlantic Council of the United States, July 2001).

20. See for example Velizar Shalamanov, “Concept and Problems for the Development of National Communications and Information Processing Infrastructure,” in *Proceedings of AFCEA-Europe Warsaw Seminar* (Warsaw: AFCEA Europe, 1993), pp.11-13.

VELIZAR SHALAMANOV is advisor to the President of the Bulgarian Academy of Sciences on national security and defense issues and Chairman of “George C. Marshall Association” – Bulgaria. Based on his experience as former Deputy Minister of Defense (defense policy and planning, November 1998 - July 2001) he serves as an advisor to the Parliamentarian Committee on Foreign Policy, Defense and Security and as Director-Strategic Studies at the Atlantic Club of Bulgaria. Dr. Shalamanov holds the title of Associate Professor on automated information processing systems and has more than 150 publications in areas of CIS architecture and development, information warfare, decision making support, national and regional security policy, military art, defense reengineering and planning.
Dr. Shalamanov is member and co-founder of the AFCEA Chapter Sofia Chapter. He serves on the Foundation Council of the Geneva Center for Democratic Control of Armed Forces. *E-mail*: vel_shalamanov@yahoo.com.

BACK TO TOP

C4ISR in Modernizing Security Sector in Bulgaria and South-Eastern Europe

Velizar Shalamanov

Keywords: security sector reform, defense reform, C4ISR, force modernization, organizational change.

Abstract: In an environment of technological revolution, C4ISR (command, control, communications, computers, intelligence, surveillance and reconnaissance) systems are given priority in force modernization. On the other side, the modernization of C4ISR, especially when implemented in interagency and international cooperation, may be an important facilitator for the overall defense and security sector reform. The focus of this article is on definition of the priority programs, model of life cycle support of C4ISR systems and its organizational dimension. We propose one possible strategy for C4ISR development in Bulgaria and South-East Europe. Organizational issues and initiatives, such as the establishment of C4 Regional Coordination Group are also debated.

full text

Author: **Atanas Zaprianov**
Title: **IT-related Challenges Facing the Bulgarian Armed Forces and Their Performance Related Impact**
Year of issuance: **2001**
Issue: **Information & Security. Volume 6, 2001, pages 23-29**
Hard copy: **ISSN 1311-1493**

IT-RELATED CHALLENGES FACING THE BULGARIAN ARMED FORCES AND THEIR PERFORMANCE RELATED IMPACT

Atanas ZAPRIANOV

Table Of Contents:

Bulgaria and NATO membership

Bulgaria is one of the South-Eastern European countries that declared its willingness to joint NATO four years ago. In April 1997, with full consensus the National Assembly (the Bulgarian one-chamber Parliament) formally approved this political decision. As a result, many political, and legislative initiatives, as well as defense reform decisions have being taken by the Government since. The Bulgarian Armed Forces modernization was predetermined by NATO's requirements for operational interoperability with the Allied Forces. Implementation of NATO's standards became very important for the achievement of the political goals. According to the Bulgarian Membership Action Plan, which is coordinated with NATO, Bulgaria has to fulfill 82 preparation objectives, called Partnership Goals. More than a quarter of them are either directly or indirectly related to the command, control, communications and computer (C4) systems. In this way, the modernization of the Bulgarian Armed Forces creates a new information environment in which the Chief Information Officer of the Ministry of Defense performs its functions. The most pressing information technology-related challenge facing the Bulgarian Armed Forces is implementing an IP router-based network, which depends on information technology policy for modernization of defense policy, doctrines, staff's structures, command and control, and communications and information systems. Advanced information technologies can greatly increase the amount of useful knowledge available to our military

organizations and improve their ability to put that knowledge to constructive use with the Allied Forces. Combining these technologies with appropriately conceived defense policy, doctrines and organizational design of the staff will provide the required interoperability.

Political environment

The first challenge of the modernization is to change defense policy. Because of its political nature policy development is an important imperative for the Chief Information Officer of the Bulgarian Armed Forces (BAF). Defense policy development is a long-term process. According to article 3(1) of The Bulgarian Law on Defense and Armed Forces "Defense is a system of activities for strengthening peace and security for preserving national values and for maintaining the Armed Forces, economy and population in readiness for actions, as well as activities in case of crisis or war." [1] Defense policy influences the information environment of the Armed Forces by helping to achieve an effective management of resources. The new defense policy also has to reflect fundamental changes, in conceptual and practical aspects of defense, as well as the reasons behind these changes. The cornerstone of the new defense policy is democratic control and civilian leadership over the Bulgarian Armed Forces.[2]

Along with our firmly stated willingness for NATO membership, policy makers must be concerned about present and future threats to national security, and the need to provide adequate military power to meet these threats.[3] The lessons learned from past reforms show that these radical steps are completely justified. Changes in military structures are very difficult to make. A joint Bulgarian and USA team conducted a study to assess the Armed Forces' reforms. Its main conclusion was that the plan we had followed until 1999 did not fit the Bulgarian strategic environment, political priorities and integration issues. [4]

A key point now is to determine measurable parameters for Armed Forces reduction, and to define proper approaches to speed up the reform. Attention is focused on the resources required to create an active force of 45,000 military personnel. In order to achieve the goals of defense policy the Government issued a program called "Bulgaria 2001", that defines the priorities as follows: building up the new model of national security and defense; creating a legislative basis adequate for a democratic society; focusing efforts on development of efficient rapid reaction forces as a part of the Bulgarian Armed Forces; defining Bulgarian's military contributions to the international community, and gradually implementing activities in accordance with The Bulgarian Membership Accession Plan to NATO. [5]

Doctrinal environment

The second challenge is to provide a conceptual and doctrinal framework for modernization. This framework is a collection of many documents, the most important of which are: The National Security Concept, The Military Doctrine, and the operational Doctrines of the Land Forces, the Air Forces and the Navy. In addition to these there are tactical doctrines, regulations, orders, governmental decisions, decisions and orders of the Minister of Defense, etc. While all these documents are important, I will focus on the first two documents.

The National Assembly of Bulgaria has approved the National Concept of Security [6] as a basic conceptual document that defines political objectives, principles, and approaches to strengthen the security and defense of the country. The National Concept of Security formulates our country's policy on equal ground common with the policy of other democracies and speeds up the preparation for NATO and European Union membership. It identifies the Armed Forces as providing for the national security and required the government to acquire the necessary resources for their mission. It is the responsibility of the government to provide stable and strong law for security, and policies for motivating military personal and creating reliable information support. Article 42 of the concept defines how important the information environment is for national security, stating, "Information guarantees national security, protecting constitutional rights and freedom of citizens, by collecting, processing and disseminating correct public and private information through advanced development of the national communications and media. It is a top priority to establish a special law for protection of public and private information resources."

The Military Doctrine [7] is the second important document for defense modernization. This document plays a key role for the implementation of an advanced information technology for modernization of the Armed Forces. According to the Military Doctrine, defense policy has to establish a military and strategic environment that allows the Bulgarian state to obtain necessary defense resources and potential to balance any threats. Furthermore, article 26 of the Military Doctrine shows that "Bulgaria comprehends NATO and European Union membership as a possibility, to share responsibilities with democratic countries for protection of common values."

The government, in accordance to the Military Doctrine, assumes its responsibility to define the place, the role and main functions of the Armed Forces in implementing the European democratic principles. Also government has to evaluate features of military strategic environment that are essential for building up national security. It is the government's obligation to define national goals and priorities in the sphere of defense policy. In addition, the government is authorized to choose directions towards building adequate military power that complies with current political realities and requirements.

The implementation of advanced information technology will help establish a system to measure the progress of reformation of the Bulgarian Armed Forces and their formation as an effective power with preventive potential, interoperable with NATO's defense system. Such technology will allow participation in peacetime cooperation, and coordination in time of crises management and in case of military conflict. [8]

Organizational changes

From a practical point of view, many military leaders have a great willingness to use information technology to overcome difficulties caused by force reduction. Because of that, the next challenge for implementation of information technology is staff structure design. The first steps have been taken since the plan for reorganization was approved in 1999. In place of the former Warsaw Pact staff organization, related to the field army-division structures, we established the corps-brigade structure with NATO's staff organization.

The General Staff of the Bulgarian Armed Forces and the staff headquarters of the services were

reduced more than 50 percent. The General Staff now has as follows: Personnel directorate, Intelligence directorate, Operational directorate, Logistic directorate, Defense and armed forces planning directorate and Communications and information systems directorate. Similarly, staffs below have been reorganized. They are not ready to operate in NATO environment until knowledge of NATO information procedures is obtained.

We must meet the challenges of implementing advanced technology in our command and control system during the modernization phase. [9] Actually, information flows were changed, but methods, procedures, applications and content are still obsolete. Furthermore, many officers are not prepared well to use advanced information systems for their job performance. Operational architecture design of command and control systems became a priority for the Chief information officer. It requires: forming teams from different branches; providing deep analyses of future warfare; learning from NATO's experience; training officers and using computer simulation models. Undoubtedly this process will be very difficult. Employing an evolutionary development and acquisition paradigm for implementing command and control capabilities will minimize the operational and cost risks associated with system implementation and will also ensure that an effective core capability will be realized in a timely manner.

Technology environment [10]

A system for high speed, reliable communications is perhaps the key enabler for realizing the full potential of future organizations that have to be established during the modernization. A high-speed strategic communications system, with reliable connectivity and robust tactical communications will be essential to network dispersed organizations and distributed but cooperative or joint operations. Some of the challenges to the strategic systems, connectivity and tactical system for one brigade include the ability to rapidly move over all territory of the country, carry large volumes of traffic and support to NATO.

Parts of the solution are found in ongoing projects for modernization of our communications infrastructure. A responsive and secure communications network must be developed to link the military headquarters across all levels of command. This is an essential enabling capability, of highest priority, to permit 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. Hence, in its fundamental form, the communications network must be able to support the timely transmission of orders and directives from higher headquarters to all subordinate forces, and be able to facilitate the timely receipt of reports, from all subordinate headquarters of the constituted military forces structure. Together, these enable the headquarters in the chain of command to monitor and control authorized military operations. To ensure timely information exchange, both secure voice service and a secure TCP/IP router-based data transmission network is required.

An advanced information system is also required at each command headquarters to provide timely and effective analytic support to the commander and his specialist functional area. Such system must enable intelligent decision-making across the entire spectrum of "informational", "organizational", and "operational" decisions. This can best be accomplished by information subsystems, organized along functional area specialists lines, which include appropriate databases and decision support tools necessary to enable the specialist staffs to accomplish their work in a timely and competent manner.

Conclusion

In conclusion, implementation of an advanced information technology for modernization of all infrastructures of the Bulgarian Armed Forces is essential. It strongly affects defense policy, doctrines, organizations and command, control, communications and information systems. In addition, it is required to support Bulgarian government speeding up priorities in military reform in order to achieve the political goal of NATO membership. Information technology will be critical because modernization over the next year is crucial for Bulgaria to be timely prepared for the second wave of NATO's enlargement.

Notes

1. Law on Defense and the Armed Forces of Republic of Bulgaria, *State Newspaper*, no. 112, 1995.

2. For the status of civilian and democratic control over the Bulgarian Armed forces refer to Plamen Pantev, Valeri Ratchev and Todor Tagarev, "Civil-Military Relations in Bulgaria: Aspects, Factors, Problems," in *Civil-Military Relations in South-East Europe: National Perspectives and PfP Standards*, ed. Plamen Pantev (Vienna, Institut fuer Internationale Friedenssicherung, 2001), pp. 31-62.

3. The two major national documents that treat these issues are the National Security Concept and the Military Doctrine of the Republic of Bulgaria. Although recent, they are under intensive debate after the September 11th terrorist acts and the subsequent biological attacks against civilians.

4. *Bulgarian Defense Reform Study*, Final Report (Washington, DC: The Office of the Assistant Secretary of Defense for International Security Affairs and U.S. EUCOM, July 1999).

5. *Cornerstones of Bulgarian Security and Defence Policy*, ed. Velizar Shalamanov (Sofia: Ministry of Defence, July 2001).

6. 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.

7. *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.

8. For details refer to Miho Mihov, "The Bulgarian Armed Forces in the Information Society," *Information & Security: An International Journal* 1, 1 (Summer 1998), 15-25; Velizar Shalamanov and Todor Tagarev, *Information Aspects of Security*, foreword by General Miho Mihov (Sofia: ProCon, 1996).

9. With the start of defense reform Bulgaria, jointly with US, conducted a comprehensive C4 Study: Command, Control, Communications and Computers Study for Bulgaria (MITRE, January 2000). It was followed by the adoption of the following documents: *Main Recommendations for the development of C4I Systems* (Sofia: Ministry of Defense, May 2000) and *Manual for C4I Life Cycle Management in the Ministry of Defense and the Bulgarian Armed Forces* (Sofia: Military Publishing House, 2000). The latter provided for institutionalizing

the Chief Information Officer.

10. Decisions in this area are influenced by theoretical developments and the experience of Bulgaria's strategic partners, most notably the United States. See for example Loren Diedrichsen, "Command & Control: Operational Requirements and System Implementation," *Information & Security: An International Journal* 5 (2000), 23-40; Charles Myer, "C4ISR Architectural Frameworks in Coalition Environments," *Information & Security: An International Journal* 5 (2000), 60-72; Roland J. Ronald, "Applying Modeling and Simulation to Enhance National and Multi-National Cooperation," *Information & Security*, vol. 3 (1999), pp. 12-24.

Major-General **ATANAS ZAPRIANOV** is Head of the Communications and Information Systems Directorate of the General Staff of the Bulgarian Armed Forces and Chief Information Officer of the Ministry of Defense. He was appointed to this position after distinguished service in the Land Forces and on joint positions. Major-General Zaprianov holds a M.Sc. degree in Communications Technology from the Bulgarian Army Academy, Veliko Tyrnovo. He is a graduate the "G.S. Rakovsky" Defense and Staff College in Sofia with a Masters degree in Military Art. In 1996 he graduated with distinction the Senior Officers' Course at the same College. Currently, General Zaprianov is taking senior executive course at IRMC at the National Defense University, Washington, DC. He is member of the Interagency Committee on Development of the Information Society and of the Armed Forces Communications and Electronics Association. Major-General Atanas Zaprianov is frequently keynote speaker to events organized by AFCEA Bulgarian Chapters, as well as to other professional conferences and seminars.

BACK TO TOP

IT-related Challenges Facing the Bulgarian Armed Forces and Their Performance Related Impact

Atanas Zaprianov

Keywords: Chief Information Officer, interoperability, command and control, C4 project management, NATO enlargement

Abstract: Development of information technology provides both challenges and opportunities for defense and security. The implementation of an advanced information technology for modernization of all infrastructures of the Bulgarian Armed Forces is essential. It strongly affects defense policy, doctrines, organizations and command, control, communications and information systems. Furthermore, it is required to support Bulgarian government to speed up defense reform in order to achieve the political goal of NATO membership. Information technology will be critical because modernization over the next year is crucial for Bulgaria to be timely prepared for the second wave of NATO enlargement.

full text

Author: **Todor Tagarev**
Title: **Prerequisites and Approaches to Force Modernization in a Transition Period**
Year of issuance: **2001**
Issue: **Information & Security. Volume 6, 2001, pages 30-52**
Hard copy: **ISSN 1311-1493**

PREREQUISITES AND APPROACHES TO FORCE MODERNIZATION IN A TRANSITION PERIOD

Todor TAGAREV

Table Of Contents:

The new security challenges in the beginning of the new century and the pace of technological innovation force politicians and planners around the world to search for ways to modernize military forces while providing for a broader spectrum of missions and tasks. For a country in transition, this search is complicated by severe resource constraints, lack of experience in market environment and relevant organizational culture. Of particular importance is the dynamics of civil-military relations that may hinder appropriate reform efforts.[1]

This article covers key issues of defense modernization and re-equipment of armed forces, including resource aspects of modernization. It is based almost entirely on the Bulgarian experience in the last three years. Bulgaria is a country in transition that differs from other countries willing to join NATO and the European Union by its excessive military and defense industrial infrastructure, inherited from the recent past. Nevertheless, the focus is on common principles; the analysis of their implementation is supported with specific examples from the experience of the Bulgarian Ministry of Defense. First, defense reform requirements are described and the necessity to introduce a rigorous defense resource management system is rationalized. Secondly, we describe organizational and procedural changes, essential for the creation of a flexible acquisition process, compatible with acquisition systems and practices of NATO and EU member countries. Next, we outline the main elements of the new acquisition planning, listing current priorities and presenting an ongoing force modernization study. The article covers also the role of research and development in modernization, as well as potential national and international cooperation activities.

Force modernization in the framework of defense reform

The task to modernize security and defense is particularly challenging for countries transitioning from authoritarian regimes to democracy and from command to a market economy. Bulgaria is one such country, which is also a fervent candidate for membership in NATO and the European Union.

Given conceptual, economic, and social problems of defense reform, Bulgaria made significant progress in the last three years. Milestone developments were the adoption of a new Concept for National Security, [2] new Military Doctrine [3] and reform plans known as "Plan-2004". The reform plans were developed under strict civilian oversight to allow balanced and gradual growth of capabilities to perform expected tasks and missions. Figure 1 represents the general defense planning framework [4] implemented in the Bulgarian Ministry of Defense. Thus, modernization plans are developed in a coherent way to meet national security requirements. Particularly, force development plans are designed so that the Bulgarian military would effectively perform 18 tasks grouped in six mission areas. Missions and tasks are listed in Annex A. [5] Plans and programs to modernize weapon systems, equipment, command and control, communications and information systems, intelligence, surveillance and reconnaissance systems (C4ISR), defense and dual-use infrastructure and building host nation support (HNS) capabilities are integral part of the defense planning process. The implementation of this general planning framework is essential in providing guidance, e.g., to build and sustain required defense capabilities accounting for resource constraints and in coordination of modernization plans with other force development activities.

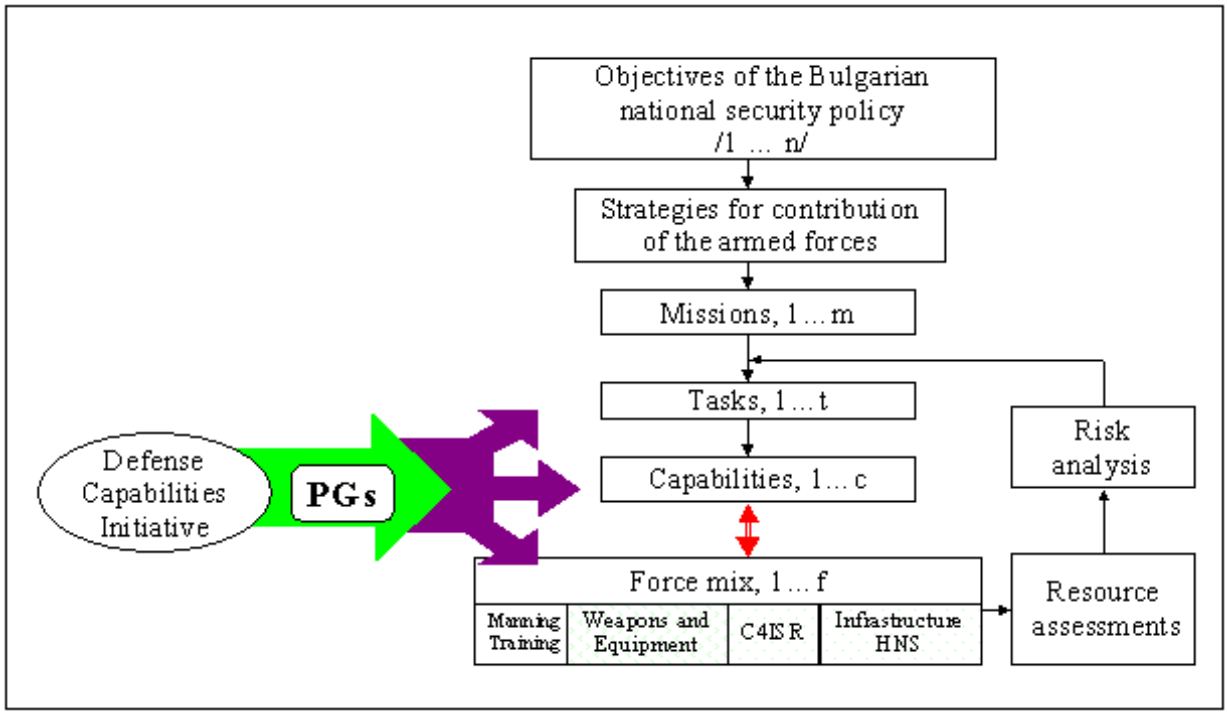


Figure 1: Modernization decisions in the defense planning framework.

Furthermore, Bulgaria introduced a rigorous defense resource management system, fully compatible with the NATO defense planning system. Finally, as one of the states striving for NATO membership in the near future, Bulgaria has its own Membership Action Plan, annual programs for its implementation and participates in the NATO Planning and Review Process (PARP). In regard to modernization, and force development as a whole, plans are designed to meet the requirements of the NATO Defense Capabilities Initiative (DCI) that during the planning process is specified in a set of Partnership Goals (PGs). Although current plans do not specifically focus on capabilities required by EU member states, their implementation would allow significant future contribution to overcome the capability gaps defined by the European Union.

Given these tools, the will of all political parties represented in Parliament and the dedication of the political majority and its Government, Bulgarian planners were able to draft mid- and long-term plans, that approximate future costs and budget levels with a reasonable accuracy. These plans are based on the assumption of sustaining the defense budget as a percentage of the GDP and are refined to better meet requirements of future NATO membership. Table 1 presents forecasted defense budget levels and forecasted budget distributions. [6]

Table 1

MOD BUDGET FOR THE PERIOD 2001-2015 BY APPROPRIATIONS (Million BGN)

	2001	*2002*	*2003*	*2004*	*2005*	*2006*	*2007*	*2010*	*2015*
Personnel cost	445.0	489.3	482.1	419.2	459.1	503.0	551.3	713.7	872.2
O&M	216.3	190.3	210.7	296.6	286.2	288.6	284.5	289.3	290.9
Investment	84.3	151.7	208.6	255.4	300.9	337.7	368.9	438.7	508.1
R&D	2.5	4.6	6.9	9.6	13.2	14.7	15.3	19.1	22.3
Budget MoD	**748.1**	**835.9**	**908.3**	**980.8**	**1059.4**	**1144.0**	**1220.0**	**1460.8**	**1693.5**

MOD BUDGET FOR THE PERIOD 2001-2015 BY APPROPRIATIONS (in percentage)

	2001	*2002*	*2003*	*2004*	*2005*	*2006*	*2007*	*2010*	*2015*

Personnel cost	59.5%	58.5%	53.1%	42.8%	43.3%	44.0%	45.2%	48.9%	51.5%
O&M	28.9%	22.8%	23.2%	30.2%	27.1%	25.2%	23.7%	19.8%	17.2%
Investment	11.3%	18.1%	23.0%	26.0%	28.4%	29.5%	29.9%	30.0%	30.0%
R&D	0.3%	0.6%	0.8%	1.0%	1.2%	1.3%	1.3%	1.3%	1.3%

This budget distribution provides for the necessary maintenance of the planned force structure, training according to NATO standards and modernizing the force to build and sustain the capabilities necessary for national defense, reasonable contribution to NATO or EU crisis response operations and significant contribution to collective defense. Strictly following reform plans, after 2004 the modernization budget [7] will amount to 25 percent of the Bulgarian defense budget. Thus, Bulgaria will meet the Common European Security and Defense Policy target figure [8] and will exceed the NATO floor for modernization spending. [9] Figure 2 shows one modernization indicator, defined as defense spending in purchasing power parity dollars per troop.

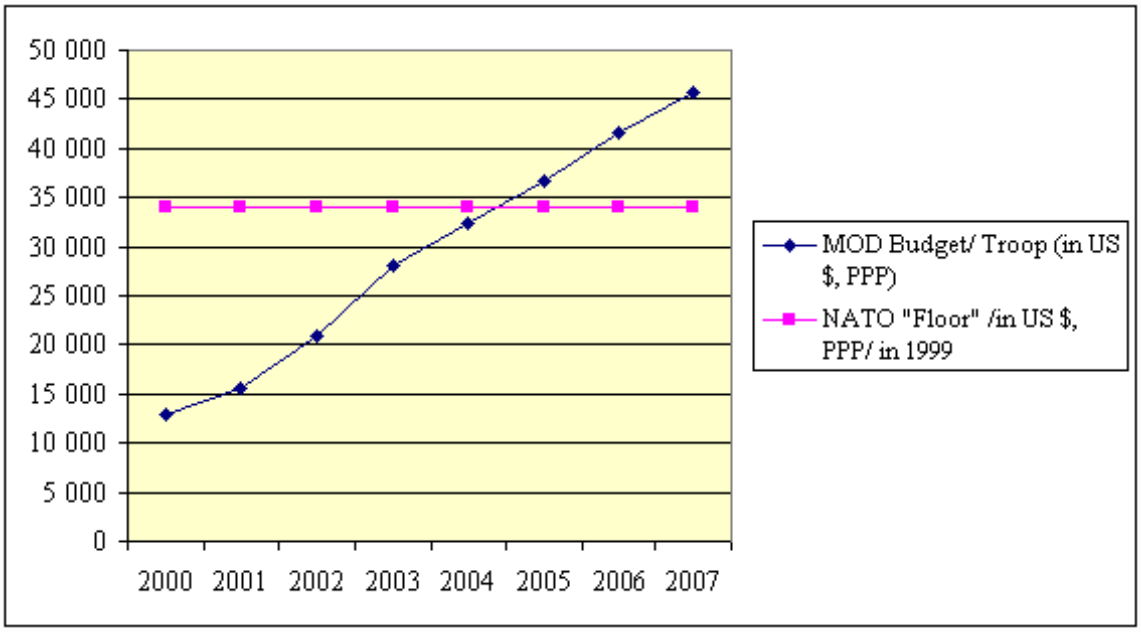


Figure 2: Modernization opportunities for the Bulgarian armed forces compared with the 1999 NATO floor. [10] The indicator is defined as purchasing power parity (PPP) dollars per troop. Calculations are based on planning figures for personnel and budget distribution.[11]

Furthermore, additional money for modernization would be available through security assistance programs and specific national programs, i.e., for harmonization of the frequency spectrum management with EU norms. These resources may amount to over 10 percent of the modernization budget. They are not included in table 1.

Thus, the comprehensive approach to defense reform and the strict implementation of reform plans provide opportunities for modernization. To use these opportunities wisely, a number of prerequisites have to be met. The experience of Bulgaria provides examples of organizational and procedural changes, considered essential for adequate modernization.

Organizational and procedural prerequisites

Analyzing problems of the existing acquisition system, the Bulgarian Ministry of Defense launched an effort to adapt the acquisition process to provide for more effective spending of taxpayers' money. Functioning closely with the resource management system, the new acquisition system (draft version from August 2001) is intended:

- To relate mission needs (capability gaps) to user/operational requirements to system and technical requirements to procurement decisions;
- To account for the life cycle cost of intended materiel solutions;
- To be transparent to decision makers, potential users and suppliers;
- To provide flexibility and efficiency;
- To be compatible with the acquisition systems of NATO and member countries.[11]

In order to support this advanced acquisition system, the Council of Ministers by its Decree # 58 of 08 March 2001 established the Armaments Policy Directorate (APD) as the principal coordinator of all modernization activities. According to the current Organic Law of the Ministry of Defense, APD performs the following main functions:

- Coordinates planning, programming and the implementation of the armaments policy;
- Develops the scientific and technological policy of the Ministry of Defense and organizes its implementation;
- Supports the implementation of the standardization, codification and state quality control of armaments and special products, their certification, as well as the certification of quality assurance systems of the producers;
- Supports the development of policy for scientific, R&D and armaments cooperation.

Furthermore, the Director of the Armaments Policy Directorate is national representative to the Conference of National Armaments Directors (CNAD) with the responsibility to coordinate planning, programming and implementation of the armaments policy.

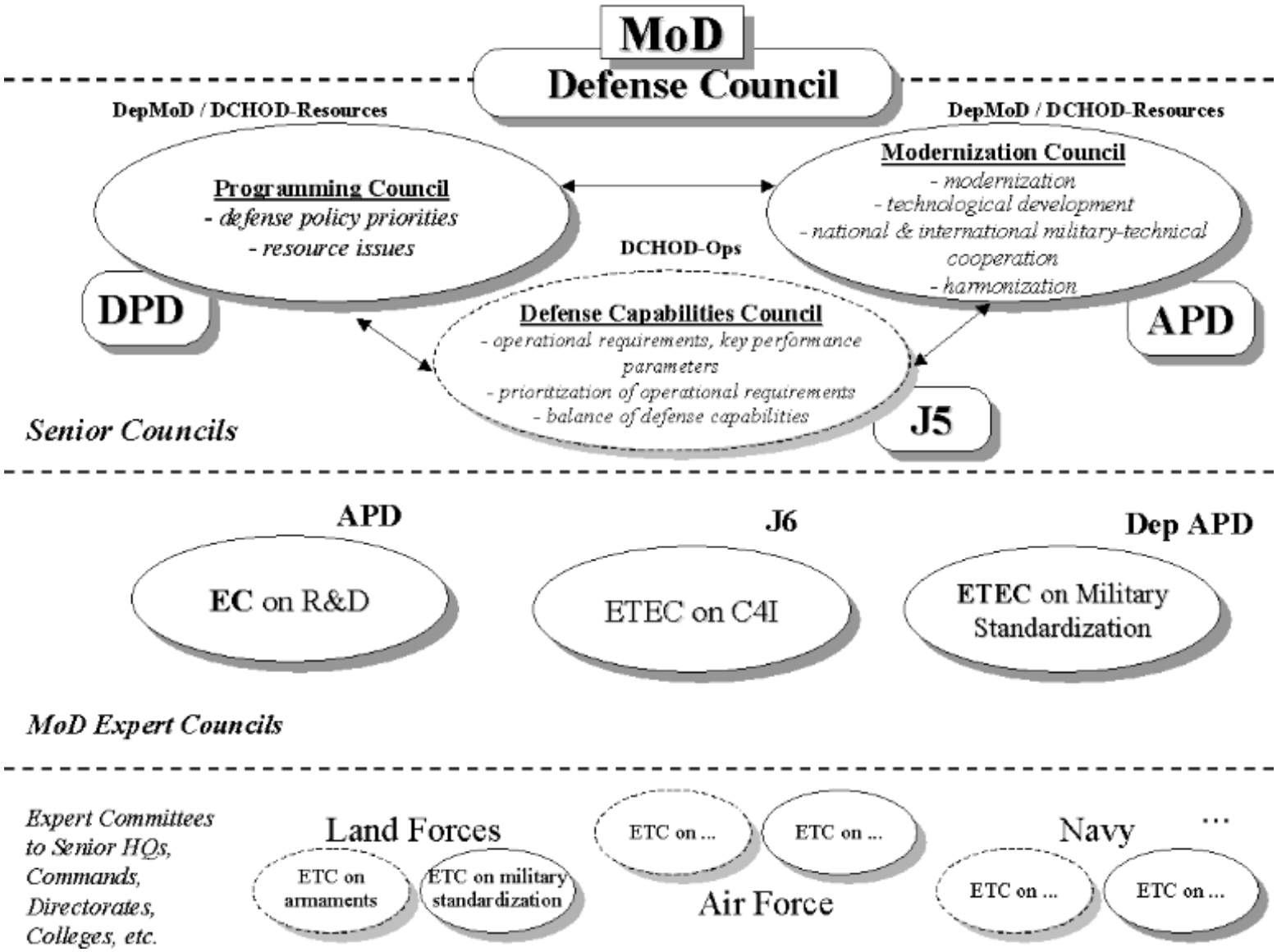
As National Armaments Director, the Director of APD coordinates the national representation in all CNAD Work Groups – NATO Army, Navy and Air Force armaments groups, the Research and Technology Organization, NATO Industrial Advisory Group, as well as the groups on acquisition practices, standardization, quality assurance, codification, etc. Thus, Bulgaria profits from the transfer of comprehensive knowledge in formulation of policies, management practices, qualification standards, technical requirements, etc.

Within the Ministry of Defense, in cooperation with the J4, J5 and J6 directorates of the General Staff, the Procurement Directorate, the Budget Planning and Management Directorate, the Executive Agency for Tests and Evaluations, and the Institute Advanced Defense Research, the APD organizes the execution of the activities at all stages of the systems life-cycle, from concept to disposal. The interaction with the Planning, Programming and Budgeting System is realized through the MoD Defense Planning Directorate (DPD) and the Defense and Force Planning Directorate (J5) of the General Staff, while the logistic support is executed through the Joint Materiel Command.

Comparing this organizational structure with the experience of NATO countries, the Armaments Policy Directorate, parts of the Procurement Directorate and the Executive Agency for Armaments and Equipment Testing and Control Measurements can be seen as a "Procurement Agency" – partner with CNAD and its working groups. Additionally, the Logistics Directorate (J4) of the General Staff and the Joint Logistics Command are roughly equivalent to a "Logistics Organization" – the partner of the NATO Materiel and Supply Agency (NAMSA).

Furthermore, a Modernization Council has been established for formulating policy in the field of armaments, equipment and infrastructure. This Council is similar in functions to the US Defense Acquisition Board. In interaction with the Programming Council and the Defense Capabilities Council (to be established), the Modernization Council gives the main directions for development of the armament and equipment for the needs of the armed forces. In this interaction, the Programming Council identifies defense policy priorities, and the Defense Capabilities Council identifies mission needs, authorizes operational requirements, provides guidance and priorities balancing planned defense capabilities.

The activity of the three Councils is supported by Expert Technical-Economic Councils on C4I Systems, on Military Standardization and on Research and Development (R&D), as well as Expert Technical Committees (ETC) on the Services level. The interaction of all these organizations is represented on figure 3.



Dashed lines represent organizations in forming. The following abbreviations are used: DPD- Defense Planning Directorate; APD - Armaments Policy Directorate; J5 - Defense and Force Planning Directorate at the General Staff; J6 – Communications and Information Systems Directorate at the General Staff; DCHOD – Deputy-Chief of Defense; EC - Expert Council; ETEC- Expert Technical-Economic Council; ETC - Expert Technical Committee.

Figure 3: Organizational support for the acquisition process.

The implementation of policy priorities under resource constraints is further facilitated by the integration of the force development and modernization in the comprehensive structure of defense programs. Currently, the programs for modernization are inherent part of the programming process in the Ministry of Defense and fall under the following program structure:

Program number:

1.6: Weapons systems and equipment for the Land Forces

2.6: Weapons systems and equipment for the Air Force

3.6: Weapons systems and equipment for the Navy

4.8: Systems and equipment for logistics and medical support

12: C4, Intelligence, Reconnaissance and Surveillance systems (C4ISR)

Program # 12 covers the introduction of advanced information technologies in education, staff training, simulation based training of troops, as well as navigation systems and systems for electronic surveillance and warfare. The development of defense and dual-use infrastructure is considered as part of the respective modernization programs of the services and the joint logistics command.

Additionally, scientific and R&D support for modernization is provided through a centrally managed program, established as main program # 10.

All future modernization programs are developed by the respective services and commands under the coordination of the Armaments Policy Directorate of the Ministry of Defense. The authorized modernization programs are part of the Program Decision Memorandum (PDM) of the Ministry of Defense. PDM has a six-year horizon and serves for budgeting for the first of the future years.

Modernization project management is carried out by Integrated Project Teams. In practice, this approach has been realized in the implementation of the Field Integrated Communication and Information System (FICIS) for the needs of the Bulgarian Armed Forces units and formations, the Air Sovereignty Operational Center (ASOC), etc. [13] The main directives for their development and the solution of problems of critical importance is done by Supervisory Boards. There is only one level of subordination between the project team and the body controlling the acquisition processes and the modernization programs – the Modernization Council.

The document information base through which the defense acquisition activities are carried out incorporates a number of additional normative and standardization documents regulating the requirements to the individual stages. Notable among them are the Law on Public Tenders, the Regulations for Public Tenders, [14] and the Instruction on Planning, Organization and Control of Logistic Support, Construction and Construction Services in the Ministry of Defense. [15] The main purpose of these documents is to provide transparency of planning and competitiveness in the implementation of procurement decision.

Rigorous planning for modernization

Since the start of the defense reform, capital investments continuously grow. Figure 4 represents the trend of increase (1 BG Lev = 1 DM), where security assistance programs are focused on the introduction of advanced communications and information systems. For the current year, the spending on R&D, overhaul, modernization and procurement of weapon systems and equipment, and construction accounts for 11 percent of the defense budget, while planned security assistance is equivalent to another 3.5 percent of the defense budget. One additional program dedicated to harmonization of the frequency spectrum with EU norms brings investments in communications systems equivalent to another 5.8 percent of the defense budget. Thus, Bulgaria already has conditions for implementation of moderate modernization programs.

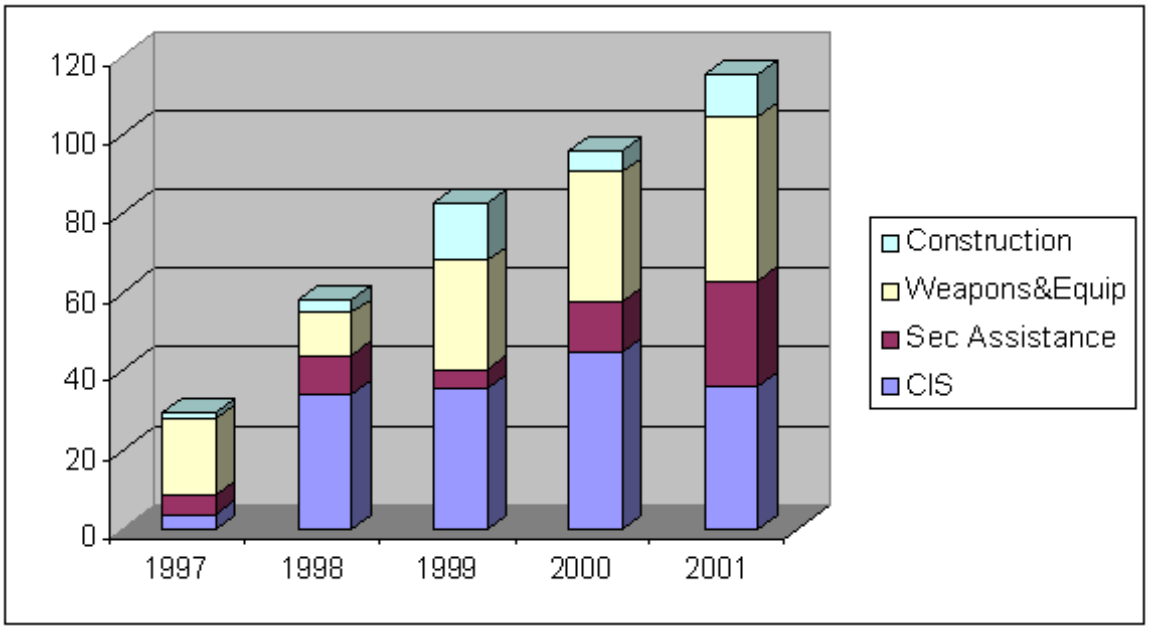


Figure 4: Capital investments, mln. BG levs

Through the Military Doctrine, in 1999 the Bulgarian Parliament defined the initial modernization priorities. According to its article 97 "… priority in the modernization of the Armed Forces is that they have the control, command, surveillance, intelligence, communications, mutual identification, computerization, navigation, (including with airspace systems, means and technologies), that would enable interoperability with the Armed Forces of the NATO countries and take into account the country's transformation to an information society."

Then, with the introduction of the planning framework and the defense resource management system described in the previous section, the following priorities for modernization were defined for the years till 2006.

General modernization priorities:

- Improvement of the C2 at international, national, strategic and tactical levels;
- Development of infrastructure for logistics support;
- Improvement of intelligence, surveillance and night vision systems;
- Developments of plans to introduce high precision weapons;
- Establishment of simulation training centers for HQs and troops, as well as simulation-based training of soldiers and crews;
- Improvement of capabilities to transport troops, equipment and supplies;
- Introduction of distance learning systems;

Priorities in modernizing Land Forces:

- Clothing, equipment and medical support for troops and HQs participating in Partnership for Peace (PfP) operations;
- Autonomous ground sensors for detection, identification and surveillance of combat equipment and people;
- Surveillance and targeting systems for artillery units;
- Modernization of short and very-short range air defense capabilities;
- Facilitate computer-assisted exercises at operational and tactical levels for all HQs and units participating in PfP operations;

Priorities in modernizing the Air Force:

- Modernization of aircraft and equipment dedicated for participation in NATO-led operations;
- Ensure full NATO interoperability of communications, navigation and supporting equipment of two military airbases;
- Start introduction of advanced ground-to-air and air-to-air missiles;
- Plan for introduction of advanced multipurpose fighter;
- Complete the build-up of an interoperable IFF system;
- Integrate the national Air Sovereignty Operations Center (ASOC) with the NATO air defense system;

Priorities in modernizing the Navy:

- Modernize the C2 system of the Navy and introduce Link-11 for frigates;
- Equip the units dedicated for peace support operations with interoperable FM and SW communications, including security equipment;
- Introduce capabilities for mine clearing at depths up to 80 meters;
- Modernize auxiliary ships;
- Introduce ship and port NATO standard equipment for fuel and water supplies;

Priorities in modernizing logistics:

- Provide NATO-interoperable C2 system for operational logistics and support;
- Equip airports, ports and railway stations for Host Nation Support (HNS) according to NATO standards;
- Provide capabilities for automatic logistics information processing and distribution among national units and regional HQs according to NATO standards;
- Establish organization and provide technical equipment for introducing F-34 fuel;
- Provide equipment for a field hospital with 80 beds and surgical capacity;

Priorities in modernizing C4ISR systems:

- Continue the priority development and implementation of C4ISR systems to achieve interoperability with NATO at strategic, operational and tactical levels;

- Build a National Military Command Center;
- Operational readiness of a field integrated communications and information system for one mechanized brigade and other units dedicated for NATO-led operations;
- Equip all units and HQs dedicated for peace support operations with commercial mobile SATCOM terminals.

For implementation of these priorities, as well as to support the development of a long-term modernization plan till 2015, the Bulgarian Ministry of Defense is currently conducting a comprehensive Force Modernization Study. This long-term plan is considered of particular importance because the next round of NATO enlargement would require the aspirants to demonstrate that they can make significant contribution to NATO's overall military effectiveness - that they will be contributors and not just consumers of security. The expectation is that the Alliance will be focusing on the capabilities and ability of candidates to contribute to NATO's old and new missions. Since Bulgaria expects invitation for membership during the NATO Summit in 2002, there is a need to begin developing a coherent, long-term plan for modernization and rearmament, including host nation support capabilities of the Bulgarian Forces well in advance of the Summit. In this regard the MoD with the assistance of the US Government performs this study as basis for the development of a long-term modernization plan for the Bulgarian Armed Forces to meet future security challenges and prepare for NATO membership.

This study builds on the final report of the "Bulgarian defense reform study," [16] "Plan for organization and development of the MoD by the year 2004," [17] the Membership Action Plan including the Partnership Goals, and the C4I study.[18] It will help the Bulgarian MoD to establish its planning priorities for defense equipment modernization and rearmament in three phases: by 2002, by 2004, and by 2015.

The study has to fulfill the following tasks:

Task 1. Equipment Modernization and Rearmament:

Building on the existing assessments of the security environment and its implications on the defense strategy and the military missions a joint Bulgarian-US team will evaluate Bulgarian force plans and structure to assess its capability to execute the military missions and tasks, with minimum risk and within forecasted resources. In this task, the Joint Team will target near-term imperatives for ensuring the national security of Bulgaria. The Joint Team will develop capabilities typical of modern Western militaries. This will include how the Bulgarian military can position itself to take advantage of the rapid advances of the military technologies. The study will also analyze the current status of the Bulgarian armed forces armament and identify, in light of the new missions, weapon systems that can be modernized and weapon systems that have to be declared obsolete, as well as ways to deal with the obsolete equipment. The findings of the study should give sufficient basis for the development of a detailed program for modernizing armaments and infrastructure.

Task 2. Impact and Implications of Defense Capabilities Initiative:

The Joint Team will examine the possible impact and implications of DCI on Bulgaria's military strategy and modernization plans. The Team will also develop an implementation strategy, outlining the key tasks that need to be carried out by Bulgaria to meet the DCI requirements. The team will identify those niche areas in which investment can bring greatest DCI returns.

Task 3. Defense Industry Development:

The Joint Team will analyze the potential of the Bulgarian defense industry in the light of its ability to support the modernization effort of the Bulgarian Armed Forces and identify possible areas of cooperation between Bulgarian and US defense industries, as well as trends for future military technology developments.

Additional to the support by the US Government, the Bulgarian Ministry of Defense is in contact with relative NATO authorities, as well as with other strategic partners to examine specific areas of modernization. The final responsibility, however, rests with the Bulgarian Government. Furthermore, the current intention is to send the Modernization Plan 2015 to Parliament that would provide guidance, exercise final authority and dedicate resources in long term.

The Modernization Plan 2015 will address several groups of issues, among them:

- *Platforms.* We expect decisions on a smaller numbers of multipurpose platforms of fewer types accounting for logistical and interoperability requirements;
- *C4ISR.* The expected focus is on integration of commercial-of-the-shelf (COTS) state-of-the-art products and dual-use technologies in joint technical architecture following the requirements of the NATO common operating environment; [19]
- *Infrastructure.* While releasing a big part of its excessive defense infrastructure, Bulgaria will plan upgrades and modernization of the remaining military and dual-use infrastructure to provide interoperability and host nation support capabilities.

- *Assets from trade.* For certain capabilities the Bulgarian armed forces would need to use assets from trade, e.g., for mobility (land, air and sea transport).

From the force modernization study and the debate on modernization we would expect a stronger parliamentarian oversight and long-term support by the People's Assembly (The Bulgarian Parliament) to provide stability and continuity of defense plans and programs, and in particular, of defense modernization programs.

Organization of defense R&D

Closely following the major decisions on defense reform, in the spring of 1999 the Minister of Defense commissioned a study on the status of Bulgarian defense R&D. From April till June 1999, the assigned working group analyzed all aspects of defense R&D and proposed a Concept for consolidation of the R&D institutes. It concluded that the existing system for defense R&D is cumbersome and inefficient and does not provide the necessary support to defense reform. For any practical purposes, in the early 1990s defense R&D organizations had not been subject to reform or accommodation to changing security requirements and declining defense budgets. At the time of the study, twelve R&DTE organizations in the Ministry of Defense employed over 1,000 people. Over 700 scientists and engineers were employed in four main institutes. Well over 95 percent of their budget was spent on personnel and basic maintenance. Research programs were heavily oriented towards narrow military R&D, with hardware developments prevalent. The organization did not provide for efficient incorporation of COTS technologies. Almost ten years after the fall of the Berlin Wall, research was still oriented towards requirements of Cold war armies and the Bulgarian defense industrial complex, relying on ever narrowing markets.

R&D Reengineering

The Concept for consolidation of the R&D institutes, approved by the Minister of Defense in June 1999, called for a national re-engineering effort, intrinsic part of the plans for comprehensive defense reform. During 1999, the Bulgarian defense R&D establishment underwent major restructuring. One consolidated organization was created out of four R&D institutes within the Ministry of Defense. Under the name "Institute for Advanced Defense Research" (IADR), it became part of the "G.S. Rakovsky" Defense College in Sofia.

IADR provides support to defense policy formulation and defense planning in developing weapon systems, organizational structures, C2, infrastructure, air defense, logistics, etc. IADR scientists participate in the formulation of requirements towards specific weapon systems and materiel and assessment of products and systems. Additionally, they provide for continuity through teaching at the "Rakovsky" College and education of doctoral students.

The budget for defense R&D is rapidly growing (see Table 1). According to the Ministerial Programming Guidance, constrained by the input of the Ministry of Finance, by the year 2005 the R&D budget will reach 1.2-1.5 percent of the defense budget – a figure typical for Western NATO member countries of similar size and ambition levels. The trend for the R&D budget is represented on figure 5.

Currently, the MoD contracts outside defense research in the following areas:

- Command and control systems;
- Computer networks;
- Decision support systems;
- Simulation in staff training;
- Information assurance;
- Implementation of space-based remote sensing technologies;
- Remotely controlled robots for hazardous environments;
- "Intelligent" / remotely controlled mine fields;
- Optical and electro-optical surveillance systems;
- Radar modernization;
- Information processing in radar systems;
- Protection from laser guided munitions;
- Passive protection of armored vehicles;
- NBC protection;
- Electro-chemical batteries.

In the beginning of 2001, the Ministry of Defense structured science and technology and R&D in a way similar to the one used by the NATO Research and Technology Organization. It covers nine broad areas: [20]

1. Systems research;
2. Sensors and sensor systems;
3. Communications and information systems technologies;
4. Modeling and simulation;
5. Transport technologies;
6. Armaments and ammunition;
7. Materiel, incl. armor, explosives, cloth, fuels, etc.;
8. NBC defense and ecology;
9. Social, psychological and medical research.

Cooperation

The Bulgarian Ministry of Defense, in coordination with the Bulgarian Academy of Sciences, universities and the defense industry, works to structure better the national defense R&D efforts and to expand the cooperation in R&D and technology development with other countries, primarily NATO and EU members or aspirants.

At the end of 1999, the Ministry of Defense signed a Framework agreement for cooperation with the Bulgarian Academy of Sciences. [21] In the spring of 2001 similar agreement was signed with the University of National and World Economics. Agreements with other leading Bulgarian universities are under preparation.

Bulgaria regularly participates in the meetings of the NATO Research and Technology Board (RTB), open for partner countries. R&D cooperation is established also on a bilateral basis. During the year 2000, a Dutch-Bulgarian Memorandum of Understanding regarding exchange of data and cooperation in defense research and technology was signed.[22] The first joint project in the area of space based remote sensing was successfully accomplished in 2000. Several new joint projects are underway.

Bulgarian research institutes have established cooperation with US defense R&D organizations, mainly through the Edison House in London. Several joint projects have been accomplished or are currently implemented. Most notable are the projects in the area light armor and naval mine warfare.

The international R&D cooperation has a driving role for reengineering Bulgarian defense research. It provides focus in conceptualizing, expanding the research area and addressing new requirements. Furthermore, it allows transfer of R&D management practices and facilitates international cooperation activities of Bulgarian universities and research institutes.

Thus, the R&D reengineering contributes to increased compatibility between Bulgaria and NATO and member countries. It provides a foundation for increased international cooperation in the future, i.e., in the area of joint procurement.

Defense modernization as driver for cooperation

During the last decade the Bulgarian armed forces have been significantly de-capitalized. No major platforms have been acquired in more than twelve years. However, national security requirements and the perspective for NATO and EU membership drive a defense reform allowing for extensive modernization. Combined with the rapidly increasing levels of training and R&D (see figure 5), modernization may have a catalyzing effect on economic development and international defense industrial cooperation.

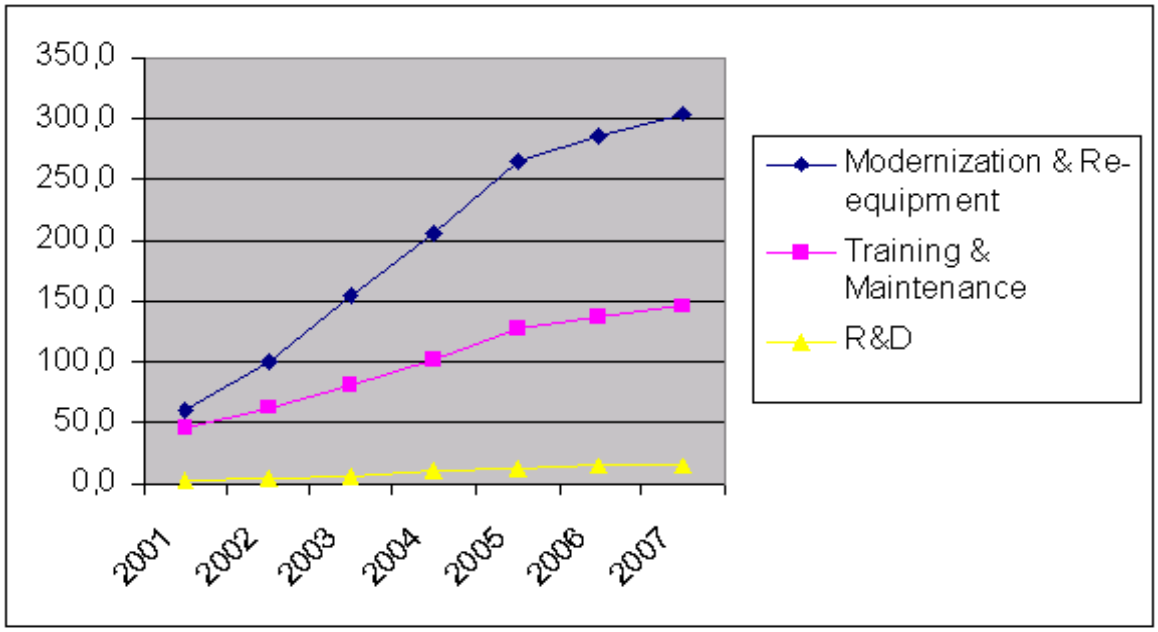


Figure 5: Economic potential of defense modernization (Resource allocations in million BG Levs).

Cooperation in the area of R&D is just one example how defense reform and modernization may contribute to economic development through technological advancement. The cooperation on a national level among the Ministry of Defense, the academic sector and the defense industry has the potential to maintain and find new niches of competitiveness on the global markets.

This cooperation will be stronger if the coordination among various Bulgarian users is improved. Given the changes in the security environment after the end of the Cold war, and in particular the rising importance of risks and threats that do not fit traditional patterns of military threats, Bulgarian defense planers pay considerable attention to the integration of various security instruments. The 1998 Concept for National Security and the 1999 Military Doctrine envision and require such integration.[23] Thus, the armed forces, the troops of the Ministry of Interior, in particular Border Police and the Gandarmerie type of units, the Civil Protection Agency and the security services need to provide complementary capabilities to undertake the full spectrum of missions and tasks in order to guarantee the national security of Bulgaria. These capabilities will be sustained in terms of organization, procedures (doctrine), training and technology, Respectively, modernization plans should account for interoperability with emphasis on all command and control functions, and when practical, commonality of weapon systems, equipment and infrastructure.

The MoD science and technology, R&D, test and evaluation programs are tools for national integration, and at the same time – vehicle for integration of the Bulgarian scientific, R&D community in the respective communities of the Western democracies.

Furthermore, the availability of compatible acquisition processes would allow exploration of various frameworks for cooperation. One obvious framework is the cooperation in South Eastern Europe building on the successful security and defense cooperation.[24] Another potential framework is among the former Warsaw Pact member countries, having similar equipment and dealing with similar heritage.

One potential start is in the area of defense technology demonstrations, using the traditional exhibition of defense industries HEMUS in Plovdiv, Bulgaria. The next exhibition is scheduled for the last week of May 2002. Several seminars are planned during the exhibition:

- Modernizing Forces to Meet the New Security Challenges;
- Second Regional C4 Conference: System Integration and Project Management;
- International Research Cooperation in Support of Force Modernization.[25]

These seminars will serve to discuss the plans for modernization of the Bulgarian armed forces, to elaborate the policy for their implementation, and to facilitate the building of strategic partnerships between users, defense industries and scientists, as well as among the countries in South-East Europe.

Conclusion

A comprehensive defense reform is under way in the Republic of Bulgaria. It requires and creates conditions for modernization of the Bulgarian armed forces. The Ministry of Defense has laid the foundations for effective force modernization that is also in the broader interests of the society.

There is still room for improvement. One major challenge is the elaboration and the implementation of consistent procedures for defense acquisition. Another challenge is the education and training of decision makers in the area of acquisition – from the member of Defense Committee in Parliament overseeing defense modernization to the officer and the civil servant who bear responsibility for a specific modernization project. Finally, Bulgaria would benefit from participation in multinational agreements on procedures and organizations for joint procurement.

Without breaking the relations with its traditional partners, Bulgaria is reorienting the modernization programs towards cooperation with future allies and partners from NATO and the European Union. Using its traditional strengths, scientific and research potential, Bulgaria needs to build strategic industrial partnerships with its future allies.

Of paramount importance is the transparency of force modernization policy. Modernization plans should be transparent to Parliament, to society, to allies and neighbors. Bulgaria needs to show that the modernization of its forces is not aimed against a particular country, but is a tool for contribution to its own security, its future responsibilities as NATO ally, and the regional stability. A similar policy of all countries in South Eastern Europe will have a stabilizing effect in the region, while the cooperation in force modernization would allow for effective development of cooperative crisis management capabilities in the best interests of the region and the international community.

Annex A

Missions and Tasks of the Bulgarian Armed Forces

M1: Peacetime functions (non-crisis situation). The Armed Forces execute tasks connected with the protection of the national integrity and sovereignty. They participate with personnel and equipment in multinational peace forces. The Armed Forces carry out activities related to the preparation of the central and local administration and the population for common action in times of crises of various nature. They participate in building dual-use infrastructure. The Armed Forces perform representative functions.

M2: Participation in the management of crises of non-armed nature. The Armed Forces participate in operations in the context of protecting the civilians and elimination of the consequences of natural disasters, industrial accidents and catastrophes. They take part in elimination of the consequences of dangerous pollution in Bulgaria and abroad. In conformity with national and international law the Armed Forces are ready to provide humanitarian assistance, to execute rescue operations on the territory and aquatory of the country and abroad whenever asked to assist the civilian authorities.

M3: Contribution to guaranteeing the internal security of the country. The Armed Forces contribute to safeguarding the national integrity, to securing the internal order through counteraction to any forces that aim at impairing the national integrity or alteration of the form of government by means of force. The Armed Forces support the civilian authorities, when requested, in operations against terrorism, organized crime, trafficking of people and drugs, illegal arms trade, smuggling technologies, strategic materials and products that may serve as a basis for construction, production or use of weapons of mass destruction.

M4: Multinational crisis response operations. The Armed Forces participate in conflict prevention, peace support operations (peace keeping, peace enforcement, peace building, etc.) and operations other than war as part of multinational contingents in accordance with the agreements and based on the mandate of an international organization.

M5: National defense. The Armed Forces defend the land, sea and air borders of the country. In times of evolving military-political crisis and a direct threat to the country, the Armed Forces may increase their forces for deterrence and defense and execute activities connected with the defense of troops, important sites and civilian population. In case of a spreading conflict within Bulgaria, under the provisions of article 17 of the Military Doctrine, the Armed Forces build-up the theatre-of-military-operations group of forces, carry out operational and, if needed, strategic deployment; they block the aggression through intensive combat activities and execute decisive counteractions in order to restore the national integrity.

M6: Collective defense. The Armed Forces and infrastructure are prepared to participate, in perspective, in collective defense according to article 5 of the Washington Treaty on the territory of the country as well as outside it.

The Armed Forces build and maintain capabilities for the execution of the following tasks:

Peacetime Tasks

> **T1**. Strategic intelligence. Independently or in cooperation and interaction with other national bodies and through exchange of information with strategic partners, and future allies, the Armed Forces maintain a picture of the situation in regions of interest to the national security for the needs of the early warning and military-political decision support;

T2. Airspace management and air sovereignty;

T3. Aquatorial control and navigation support;

T4. Participation in the implementation of international treaties and initiatives related to the enhancement of confidence and cooperation in the military field;

T5. Participation with personnel and equipment in multinational peace forces;

T6. Ceremonial functions;

T7. Transportation of (VIP) statesmen;

T8. Participation in the preparation of the population, national economy and wartime reserves for protection in crises of different nature and preparation of the country for defense;

Crises of non-armed nature

T9. Protection of the population in natural disasters, industrial accidents and catastrophes;

T10. Humanitarian assistance in international humanitarian crises;

Internal Security

T11. Support of the civilian authorities in counteracting non-military threats of (potentially) armed character: illegal traffic of people and weapons, drug traffic, organized crime and in maintenance of law and order;

Crisis response

T12. Participation in peace-support operations;

T13. Search and rescue;

T14. Personnel evacuation from crisis areas;

National Defense

T15. Information superiority (Military Doctrine, article 62);

T16. Conducting of defense operation in line with article 17 of the Military Doctrine;

T17. Territorial defense;

Collective Defense

T18. Participation (following NATO accession) in defense operations of the allied forces.

Notes:

1. Plamen Pantev, ed., Civil-Military Relations in South-East Europe: A Survey of the National Perspectives and of the Adaptation Process to the Partnership for Peace Standards (Vienna: Institut fuer Internationale Friedenssicherung, 2001). The full text is available at http://www.isn.ethz.ch/isis.
2. National Security Concept of the Republic of Bulgaria, State Gazette 46 (22 April 1998). Available full text in English at http://www.md.government.bg.
3. 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.

4. Tagarev, T., "Transparent Defence Planning for Effective Democratic Control," in PFP Planning Symposium (Oberammergau, Germany: January 2001). Slides are available at http://www.isn.ethz.ch/pfpdc/e_index.htm.
5. Velizar Shalamanov, ed., Cornerstones of Bulgarian Security and Defence Policy (Sofia: Ministry of Defence, July 2001).
6. Shalamanov, Cornerstones.
7. The figures for “modernization” and “investment” differ. According to Bulgarian legislation, modernization, re-equipment and new defense infrastructure spending constitutes only part of the investment budget. The latter further includes overhaul of weapon systems, equipment and infrastructure, as well as building of barracks, housing, etc. The adoption of common NATO definitions is strongly recommended.
8. Gilles Andreani, Christoph Bertram and Charles Grant, Europe’s Military Revolution (London: Centre for European Reform, March 2001).
9. Thomas S. Szayna, NATO Enlargement, 2000-2015: Determinants and Implications for Defense Planning and Shaping, RAND Report MR-1243-AF (RAND Corporation, 2001). Available at http://www.rand.org/publications/MR/MR1243/
10. Szayna, NATO Enlargement.
11. Review of Force Structures in Implementation of Partnership Goal G 0028, Preliminary Report for Consultations with NATO (Sofia: Ministry of Defense, 28 May 2001).
12. See for example The Acquisition Handbook: A Guide to Smart Procurement, Edition 3 (London: Ministry of Defence of the United Kingdom, June 2000); US Acquisition System, DoDD 5000 series; Defence Materiel Selection Process: The Outlines for Procurement of Materiel (The Hague: Directorate-General for Materiel, Ministry of Defence of The Kingdom of the Netherlands, 1999).
13. See the articles by Stoyan Balabanov, “Field Integrated Communication and Information System for Bulgarian Land Forces” in this volume, and by Stoyan Avramov, “ASOC and C4I Systems Integration” in volume 7, 2002.
14. Law on Public Tenders, State Gazette 56 (22 June 1999).
15. Instruction on Planning, Organization and Control of Logistic Support, Construction and Construction Services in the Ministry of Defense, Instruction # 1 (7 February 2001). Available in Bulgarian at http://www.md.government.bg.
16. Bulgarian Defense Reform Study, Final Report (Washington, DC: The Office of the Assistant Secretary of Defense for International Security Affairs and U.S. EUCOM, July 1999).
17. Recommendations for the development of the Plan for Organizational Evolvement of the Ministry of Defense and the Armed Forces until the year 2004 (Sofia: Ministry of Defense of the Republic of Bulgaria, May 1999).
18. Command, Control, Communications and Computers Study for Bulgaria (Hanscom AFB: USAF ESC/MITRE, January 2000); Main Recommendations for the development of C4I Systems (Sofia: Ministry of Defense, May 2000).
19. Details are provided in the article by Velizar Shalamanov in this volume.
20. Tagarev, T., "Organization of Scientific Research and Development in the Interest of Defense," Military Journal 108, 1 (2001): 35-45.
21. The Bulgarian Academy of Sciences includes approximately 70 institutes and laboratories with over 8,000 personnel. Approximately 3,500 of these are scientists. In order to improve coordination of its defense and dual use research activities, in the spring of 2001 the leadership of the Academy created a Center for National Security and Defense Research <http://www.icsr.bas.bg/cnsr/>.
22. Memorandum of Understanding between the Ministry of Defence of the Republic of Bulgaria and the Minister of Defence of the Kingdom of the Netherlands regarding exchange of data and co-operation in defence research and technology, August 2000.
23. Confirmed through the list mission and tasks in the Defense Programming Guidance 2002-2207, given also in the Annex.
24. See for example G•l Sosay, “Regional Security Challenges and Opportunities in the Balkans,” in International Seminar on Regional Security Challenges and Opportunities in the Balkans: Towards Harmonized Perceptions and Cooperative Security Studies (Istanbul: Center for European Studies, April 2001). Available electronically at http://www.isn.ethz.ch/pfpdc/e_index.htm.
25. Current information about the seminar will be available at the Web site of the Center for National Security and Defense Research at the Bulgarian Academy of Sciences.

Since May 2001 Dr. **TODOR TAGAREV** is Director of the Armaments Policy Directorate of the Bulgarian Ministry of Defense and National Armaments Director. Prior to that, he was the first Director of the Defense Planning Directorate since its establishment in May 1999. In 1982 he graduated from the Bulgarian Air Force Academy with M.Sc. degree in Automatics (Aviation Weapon Systems and Missile Technology) and in 1989 received a Ph.D. degree in control and systems research from the ‘Zhukovsky’ Air Force Engineering Academy, Moscow, Russia. Dr. Tagarev is a 1994 Distinguished Graduate of the US Air Command and Staff College and 1994 Distinguished Young AFCEAn. He holds Associate Professorship and is a Senior Research Associate of the Institute for Security and International Studies, Sofia, Bulgaria. Dr. Tagarev is Managing Editor of ‘*Information & Security. An International Journal*’ and member of the Editorial Board of *‘Military Journal’*. He has published extensively in the areas of defense planning, information aspects of security, computer studies, modeling and prediction of complex processes, including security processes and defense related issues.

BACK TO TOP

Prerequisites and Approaches to Force Modernization in a Transition Period

Todor Tagarev

Keywords: Force planning, force modernization, defense acquisition, NATO enlargement, partnership goals, defense capabilities initiative, defense R&D

Abstract: The new security challenges, in particular the challenges stemming from the wave of terrorist attacks and massive use of biological threats in September 2001, require novel ways of organizing and modernizing military forces. In the beginning of the Twenty First century militaries have to perform a broader spectrum of missions and tasks in cooperation with other agencies and other countries. For a country in transition, the search for effective modernization is complicated by resource constraints, lack of experience in market environment and relevant organizational culture.

This article describes the application of common principles in modernizing Bulgarian military. It describes defense reform requirements with emphasis on the necessity to introduce rigorous defense resource management. The major challenge is to implement organizational and procedural changes, essential for the creation of a transparent, flexible acquisition process, compatible with acquisition systems and practices of NATO and EU member countries. The article provides details on the main elements of the new acquisition planning, listing current priorities and presenting an ongoing force modernization study. It covers also the role of research and development in modernization, as well as potential national and international cooperation activities.

full text

Author: **Daniel F. Wiener II and John Courtien**
Title: **Bulgarian Information Network: Command Information Infrastructure for the Future**
Year of issuance: **2001**
Issue: **Information & Security. Volume 6, 2001, pages 55-68**
Hard copy: **ISSN 1311-1493**

BULGARIAN INFORMATION NETWORK: COMMAND INFORMATION INFRASTRUCTURE FOR THE FUTURE

Daniel F. WIENER II and John COURTIEN

Table Of Contents:

INTRODUCTION

Although the demise of the Warsaw Pact in 1989 has changed the landscape of the world, rogue states, terrorism, natural disasters and other crisis situations remain as hostile threats to all nations. Terrorist bombings (including weapons of mass destruction and disruption), earthquakes, floods, environmental disasters and a host of other catastrophes may cause devastation with loss of lives and considerable property damage. Terrorist cyber attacks and organized crime may cause devastating economic harm. At the same time, nations are faced with defense of their homeland against new threats from rogue states. The resulting future challenges to the Bulgarian government include: strategic assets, fixed bases being at risk; maritime forces in the littoral being at risk; and a growing incidence of urban conflict.

In response to these situations, nations need to effectively apply national resources to alleviate the consequences of rogue states, terrorism, disasters and crises. These resources typically include a host of civil and military units that may be called upon to provide assistance in the face of crisis situations. In order for these forces to respond to crisis situations in an efficient manner, two fundamental requirements are:

- Availability of information regarding crisis situations and military/civil resources readiness, and
- Coordination with the many national organizations and agencies involved in crisis management.

This paper addresses the operational aspects of an information infrastructure intended to assist the Bulgarian Ministry of Defense (MoD) in coordinating with other national (and perhaps regional) organizations dealing with crisis situations and also in applying military/civil forces in execution of military/crisis management responsibilities.

BACKGROUND

To support the military/civil forces of today, as well as by 2010 and beyond, interoperable, assured, end-to-end networks for information and Command and Control (C2) transport are vital. All information and data are required to be available end-to-end to support whatever mission requirements exist regardless of environment. Concurrently, the exponential growth of the internet/world-wide web has resulted in the convergence of the public switched networks and the routed Internet Protocol (IP) networks, as well as causing the inclusion of functionality on/within the "network." The growth of the internet/world-wide web is also resulting in exciting new capabilities and services, including data mining, smart data push, etc. that have applicability for the battlefield commander/crisis manager, e.g., an increased ability to operate faster with increased fidelity in the preparation of the Situation Assessment/Common Operating Picture, as well as faster synchronization of operations. Add to this, the emerging wireless internet/world-wide web capabilities and the advances in

software-programmable, packet switching radios provide the foundations for a commercial technology-driven 21st century Command Information Infrastructure.

OVERVIEW

The Bulgarian Information Network (BIN) is a vision for achieving total information ubiquity – hence, information superiority. The BIN is focused on both the war fighters, law enforcer's and crisis manager's need for assured information.

This envisioned globally interconnected infrastructure would provide the framework for an end -to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on-demand to warfighters/crisis managers, policy makers, and support personnel. The envisioned BIN includes all owned and leased communications and services, data, and security services and other associate services necessary to achieve an Assured Communications Infrastructure. The BIN supports all MoD, related Intelligence Community, Law Enforcement and Crisis Management missions and functions (strategic, operational, tactical and business) in war, crisis and in peace.

The BIN would be a secure, data distribution backbone. It is intended for all levels of military action/crisis management in coordinating military/crisis management activities. The infrastructure will provide connectivity with national military and civil information sources and with national military and civilian agencies and organizations involved with military operations/crisis management. Specifically, the BIN is envisioned as structured to provide the infrastructure and backbone to:

- Collect and correlate information on the scope and nature of a crisis. This includes situational information, status of forces and resource information.
- Provide means to consolidate information received from disparate sources into a comprehensive picture for decision support at the highest national level.
- Provide the capability to coordinate crisis response activities with other national organizations involved in the crisis management process.
- Provide a vehicle for collaboration with regional/coalition partners in cases where crises cross national boundaries.
- Provide a mechanism for communications and order dissemination to relief units.

As such, it is a single secure grid providing seamless end-to-end capabilities to all warfighting, national security, and support users.

BULGARIAN INFORMATION NETWORK (BIN)

The Past

Throughout the 1990s, Government leaders made a conscious decision to modernize defense forces and develop e-Government capabilities and services. These decisions were driven by the increased expectations fostered by the Internet and the desire to improve combat efficiencies with a smaller force structure, as well as the goals of integration into the European Union (EU) and the North Atlantic Treaty Organization (NATO). The necessity of this decision was amply demonstrated during South East Defense Ministers' (SEDM) discussions on humanitarian and law enforcement, and discussion for NATO accession. In an age where split-base, joint, and combined operations are the rule, robust information systems and services providing communications support to warfighting forces, and Government/law enforcement personnel during all phases of an operation are crucial and necessary in fulfilling the country's modernization objective.

The Future

In addition to a growing computer literate population, the Government of Bulgaria is faced with natural disasters and other crisis situations that remain as hostile threats. Devastating earthquakes, floods, environmental disasters and a host of other catastrophes may cause devastation with loss of lives and considerable property damage. In response to these situations, nations need to effectively apply national resources to alleviate the consequences of disasters and crises. Effective battle command will be a dominant aspect of future conventional battlefields, and is highly dependent on the actions of quality soldiers, sailors and airmen, and competent leaders. Success will be achieved largely through the ability to rapidly move, process, and share information and to acquire and share *a common, relevant picture* of the battlefield as it pertains to soldiers, sailors and airmen's and leaders' interests and needs. The ability to gain a situational understanding of the battlespace is imperative and will be inextricably tied to, and dependent upon, the capabilities of future communications support systems. In both cases these resources typically include a host of civil and military units that may be called upon to provide assistance in the face of crisis situations.

Personnel and leaders will be called on to continually adapt tactics, techniques, and procedures in dynamic environments and under conditions ranging from conventional warfare to law enforcement to humanitarian aid. Communications support doctrine and subsequent

development of future information systems must provide communications leaders latitude and flexibility to adapt to various environmental and operational conditions and employ communications systems as needed to support Government forces.

There are two fundamental requirements in order for these forces to respond to crisis situations in an efficient manner:

1. The availability of information regarding crisis situations and military/civil resources readiness, and;

2. Coordination with number of national organizations and agencies involved in the activity.

This paper addresses the operational aspects of an information backbone system intended to assist Bulgarian Government organizations in coordinating with other national (and perhaps regional) organizations dealing with military, law enforcement and crisis situations, and also in applying Government personnel in execution of crisis management responsibilities as agreed with other national agencies and organizations.

Overview

The BIN provides a mobile, secure, survivable, seamless communications backbone to support data integration, information processing, and display, i.e., command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR). It is intended to be used at the Government Minister-level through the mobile/maneuver unit and support senior Government decision-makers in coordinating military, law enforcement and crisis management activities. The system will interface with national military Service Headquarters, with national military and civil information sources and with national civilian agencies and organizations involved with crisis management. It may also be used to support regional, allied and coalition coordination in the event of situations that affect large regional areas.

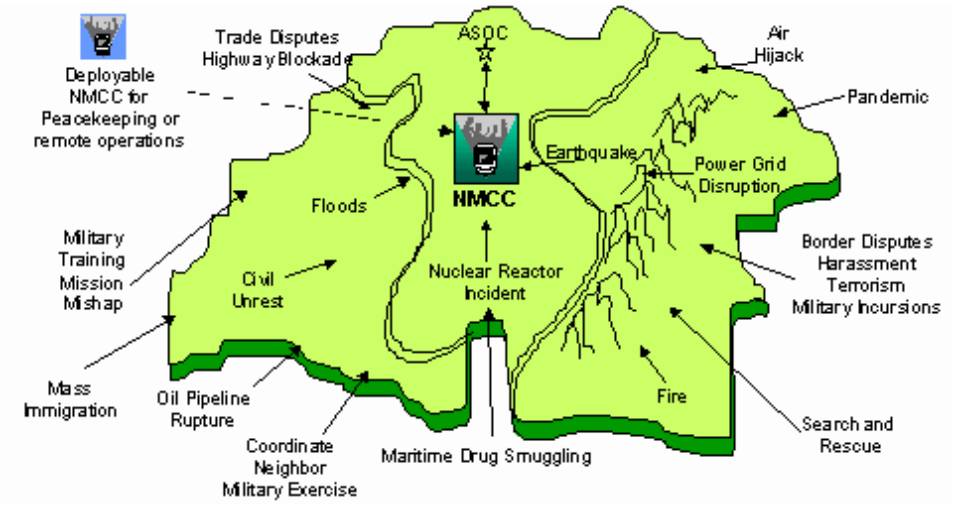


Figure 1: NMCC Support to Crisis Management Operations

Figure 1 shows different scenarios in which the National Military Command Center—one of the users—can provide support to manage crisis response operations.[1]

On a military basis, the BIN supports unit task organization and real-time reorganization of battlefield support elements - a vital enabler for future operational concepts. The BIN will allow Joint Forces and Service commanders and other network users, at all echelons, to exchange information internal and external to the theater, from wired or wireless devices, network appliances (Internet-like capability), or video terminals. BIN connects all users from the theater to the maneuver unit, to joint and multinational elements. The BIN employs a combination of transport options to provide robust connectivity to all users.

In summary, the BIN's infrastructure will provide commanders/leaders and other users the ability to simultaneously communicate via voice, data, and video at levels of security wile on the move by leveraging software programmable radios, wide-band digital radios, and wireless local area network (LAN) technologies.

Existing Shortcomings

Operational concepts have changed significantly and crisis manager, law enforcer, warfighter requirements for a mobile communications infrastructure have grown beyond the scope of the existing communications networks. Soviet-based and current commercial services are not capable of supporting the Government's needs. These services were designed to support a command and control/crisis management and support service that relied heavily on voice, small data files and short text messaging. Today's Government organization depends on a much broader spectrum of information services: video, graphics data, imagery, collaborative planning tools, remote interactive

battlefield/crisis management operating systems, and distributed databases.

The battlefield/crisis management command and control systems, service support systems, military intelligence and electronic warfare & sensors (IEW&S), and other proponent systems require a robust communications network for passing information. Without the increased capacity, speed of services, network services, and network infrastructure BIN provides, these systems will not be able to operate as designed in today's bandwidth-constrained environment.

Crisis Management

The BIN must support crisis management operations for military, law enforcement and civil activities. These operations can be separated into the four distinct periods as shown in Figure 2.[2]

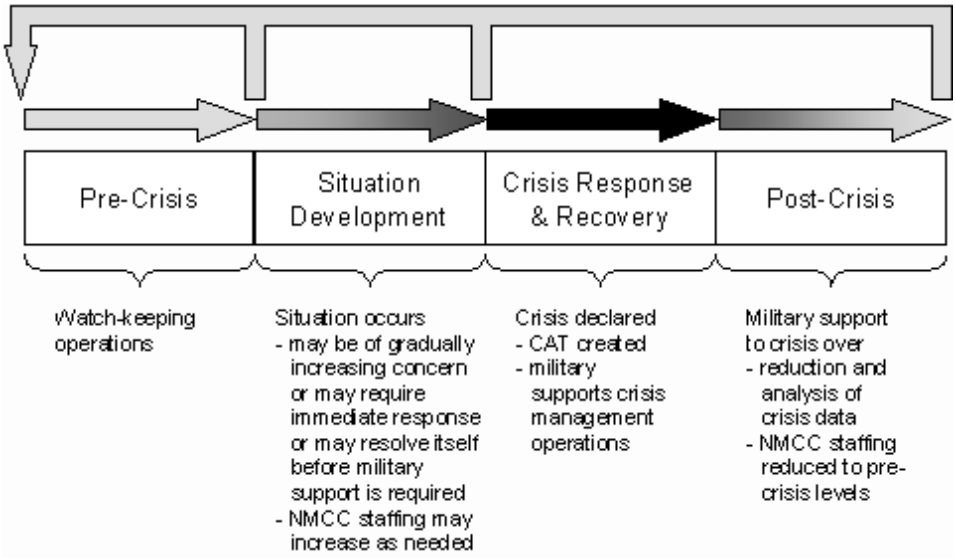


Figure 2: Crisis Management Periods

Other Warfighting Concepts

The Bulgarian Land Forces C4 Concept of Operations describes a battlespace where operations are distributed, simultaneous, and heavily reliant on information technology. Improved situational awareness, sensor to shooter capabilities, and C2 are just a few aspects of information dominance that BIN enables. Bulgarian Land Forces C4 Concept of Operations High-Level Operational Concept Graphic (Figure 3) shows the various echelons that are to be addressed. From the BLF HQ level (*Strategic/ National*), where the Command Information System (CIS) addresses the BLF Headquarters level and all C3 interfaces between the BLF HQ and all Joint and MoD-level Agencies; through the BLF Regional Force level (*Strategic, Theater and Operational*), where the CIS's focus will be on C2 high-level Operational Planning Management and Sustainment of the Field Forces; to the Corps and Brigade level (*Tactical*), where the CIS will be structured to have the same Force-oriented functionality, but will be more mobile and near-real-time in nature.[3] The High-Level Operational Concept Graphic shows a view of the Brigade organizational and operational laydown and deployment in greater detail due to its linchpin status in the BLF organization, including the Brigade-level tactical Internet. At the high level, this shows the type of platforms that will be used and the communications functions of the different types of platforms.[4]

Interoperability

The BIN is required to provide mobile, secure communications between numerous military, law enforcement and civil agencies. The required baseline interfaces are identified generically as:

- Military Services and Agencies and systems, including the entire spectrum of the Land Forces, Air/Air Defense Forces and Naval Forces from the National Military Service HQs to each other, as well as their subordinate commands;
- National Agencies and Systems, including government organizations such as the office of the President and ministries (Senior Leadership) involved with national Internal Affairs, Foreign Affairs, Transportation, Telecommunications, Health, Agriculture, Industry, etc., as well as agencies dealing with Civil Protection (fire guard, border guard, etc.);
- Public Information Agencies, including news services such as Cable News Network (CNN), the British Broadcasting Corporation (BBC), and local television and radio stations;
- Regional and Coalition Organizations, including nations participating in a crisis response on a bilateral or multilateral basis between specific countries in the region or in a coalition environment, e.g., NATO;

- Deployed command centers, including centers for military, law enforcement and crisis management operations; and
- National Military Command/Crisis Management Center(s) Deployment/ Redeployment.

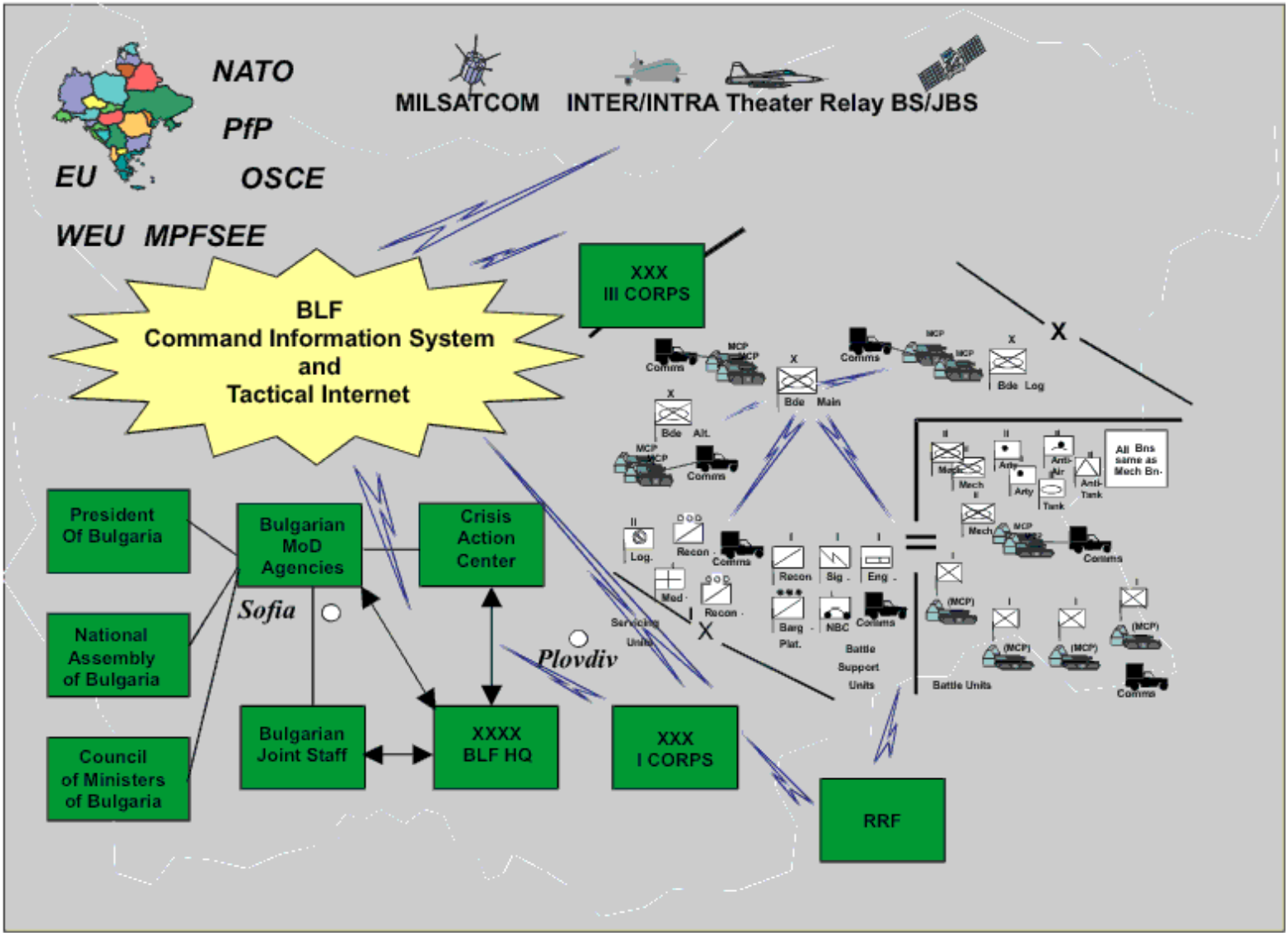


Figure 3: High-level Operational Graphic

In general, these interface categories are notional – given the stage in their planned automation. As such, they should be viewed as a starting point for the development of specific interface requirements for the BIN. These organizations/systems are divided into two groups: classified information sources, i.e., providers/receivers of classified information, and unclassified information sources. National military service HQs, service operations centers, national military information systems and the optional deployed command centers are considered classified sources. National and public information agencies and systems are considered unclassified sources. Regional and coalition organizations are considered coalition-sensitive sources and are implicitly connected to the regional WAN.

BIN Elements

The key to any C2/crisis management center is the capability to receive and correlate information concerning crisis situations and the status of resources to provide relief and the ability to transmit directives to apply resources where needed. It must be possible to move information within the entire area of operations to organize and display received information. It must also be possible to transfer information to/from external organizations in order to collaborate on crisis relief actions and coordinate resource allocations. A rich communications suite, both voice and data, is required to satisfy this need. As such, it is essential that the communications infrastructure is robust, ensuring as much as possible that connectivity is available during crisis situations. Operational requirements exist for:

- Voice, data, and video transfer;
- Classified, Sensitive But Unclassified and clear transmissions;
- External communications with mobile command centers;
- Communications within the host nation and with regional partners.

In order to satisfy such diverse requirements, several components must be combined. A classified LAN is provided for communications between command centers. A coalition-sensitive LAN is used to support connectivity to a regional WAN.

The BIN elements will be owned, operated, and maintained by both communications and non-communications units. Key components include switching, routing, transmission, information assurance (IA), information services, and network management systems. These components form a communications network infrastructure that provides a means for deployed Government organizations to transfer information in the form of voice, video, data, and imagery.

The BIN supports the mobile Government operations by providing a survivable, tactical, wide-area communications network that operates in complex, rolling, and urban terrain. It will extend data connectivity to forward elements and route information efficiently anywhere in the country, and will reduce the traditional communications presence on the area of operations. The BIN's design will facilitate the fielding of smaller, lighter, more deployable communications equipment. Thus, BIN will reduce tactical communications node terrain footprint by 50 percent and reduce the communications organizational structure in a division by 15 percent to 20 percent.

BIN's connectivity provides commanders' access to Joint, North Atlantic Treaty Organization (NATO), and commercial networks. These systems enable commanders and leaders to have a virtual presence, "see and understand" their areas of operations, achieve situational awareness, and exercise C2. BIN also provides C3 on the move capabilities by integrating some of the same functionality found at higher echelons into Warfighter platforms. Wide-band networking radios will provide the primary transport for the exchange of data.

BIN Notional Implementation

A notional implementation is shown below - where a push-to-talk/narrow-band radio environment has been replaced with a network radio, a la the AN/VRC-99 Joint Tactical Radio System. This example shows how network radios can transform a communications network into an information grid over which it is possible to provide "web-style" application functionality, as well as terrestrial/commercial network interfaces.

This envisioned BIN extends from the post, base, camp, and station, through the strategic networks, to the "last tactical mile." The last tactical mile extends to the Service weapons and sensor platforms. The bridge between the strategic and tactical networks is envisioned to be T-l ports. T-l ports would provide deployed communications networks access to strategic networks and the services, and data that those networks have to offer, e.g., secure and nonsecure telephone, data, and video teleconferencing networks. This would allow the deployed warfighter in a Navy ship, Army division, or Air Force wing access to data stored on these strategic networks, and provide a means to push information to strategic planners. As the more forward "networked sensors" need to move data and information in real-time, it would make the communications component more critical to operational success. Doctrine and policy will dictate access, but the information and data will be available for push or pull.

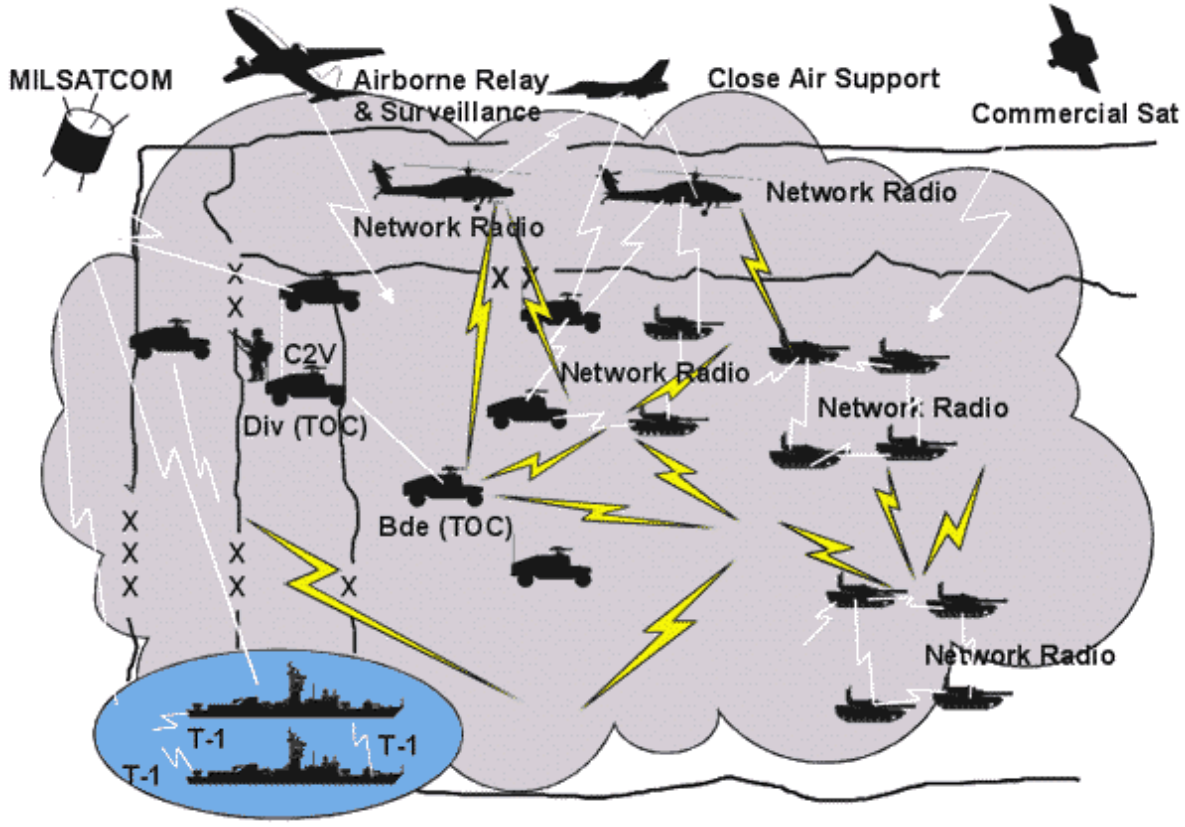


Figure 4: A notional implementation

Other Issues

Security

The BIN provides secure communication transport services and will have multiple security environments. One security environment will support the BIN's Unclassified (U) and Sensitive But Unclassified (SBU) information processing requirements and will be interconnected with the Internet and other Government networks. This U/SBU environment is referred to as the Unclassified LAN. The security measures for this Unclassified LAN will be based on best commercial practices and COTS components. The second security environment will support the BIN's classified information transport requirements and will be interconnected with classified (and, if desired, unclassified) national and allied systems using appropriate security mechanisms. Military grade cryptography should be used to protect all external classified communication links. This classified environment is referred to as the BIN's Classified LAN. Both of these environments will be operated in the System High mode and the highest level of classification handled by the BIN's Classified LAN.

The following paragraphs provide a more detailed description of the security features of each environment and outline a conceptual approach for providing information assurance (IA) for the BIN. Physical, technical, communications, personnel and other security aspects are addressed. For NATO-related operations, it is important to remember that the document *CM(55)15 Final* establishes a minimum set of security requirements for national facilities processing, storing, transmitting or otherwise handling NATO classified information.

Information Assurance

BIN is not designed to counter a specific threat capability; however, certain security components are designed to protect BIN from the Information Warfare (IW) threat. IA components are part of the BIN "Defense in Depth" concept, which protects the information network from attempts to penetrate the network to obtain, disrupt, or manipulate network data. BIN's Defense in Depth allows simultaneous access and processing protection for users at different security levels. Additionally, the network must support Classified, and Sensitive Unclassified Information (SUI) in accordance with the requisite security policy requirements. Mechanisms must be available to control, filter, and protect both incoming and outgoing connections to the network, e.g., boundary protection, network perimeter, and internal intrusion detection systems.

Training

There shall be two types of training: BIN systems and BIN network management. The initial training will be by the BIN contractor. The contractor will prepare courses for system operations training, system/network administration training, security administration training and system maintenance training. The courses will assume that the personnel to be trained already have basic network technology/communication systems skills and familiarity with IP networks. The contractor will conduct formal training courses. Each class (operator, administrator, maintenance) should last two weeks. The contractor will conduct training for designated Government trainers. Continuation/replacement training will be conducted by these designated trainers. An option shall be made available for on-line training and help functionality will be provided to support the user in learning and using the BIN system.

Sustainment

The BIN will be contractor supported by trained technicians. The contractor will provide software maintenance for all delivered software, databases, and support software, and will provide maintenance for the BIN hardware items, including factory Repair and Return. The contractor will provide a detailed plan for transitioning hardware maintenance and on-going software administration after a defined warranty period has expired. In country resources will then be responsible for the sustainment of the BIN. The BIN program may include additional-cost options for contractor software maintenance beyond the two-year maintenance period. The BIN shall be designed so that there is no specific limitation on life cycle, and because of its modular nature, specific components can be upgraded independently without compromising the system design. In order to facilitate connectivity with other allied/coalition networks, any plans for upgrading BIN components should be coordinated with allied/coalition partners.

Summary

The Bulgarian Information Network (BIN) is the globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to Government, warfighters, law enforcement, policy makers, and support personnel. The BIN includes all owned and leased communications and computing systems and services, software (including applications), data, security services and other associated services necessary to support mobile, Government information operations. The BIN connects the Government personnel to capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites) and provides interfaces to coalition, allied and coalition users and systems.

From a Ministry of Defense basis, BIN is the Services' communications support concept for integrating foxhole to sustaining base communications and information services that support the Services' Command, Control, Communications, Computers Intelligence,

Surveillance, and Reconnaissance (C4ISR) requirements to warfighting command posts from theater boundaries down to maneuver battalions. BIN also supports non-Defense Bulgarian Government users by providing voice, data, and video services to remote locations throughout Bulgaria. The goal is to dramatically increase the capacity and velocity of information distribution throughout the country.

Defense operational requirements for communications support are derived from the development and fielding of warfighter information systems such as the Battlefield Command System and information services such as collaborative planning, information assurance (IA), and battlefield video teleconferencing (VTC). Non-Defense operational requirements are derived from information services such as collaborative planning, information assurance, and operational video teleconferencing (VTC). The throughput requirements and speed of service demanded by these operational requirements have made the current communications networks obsolete.

Notes:

1. For additional information refer to Roland J. Ronald, "Applying Modeling and Simulation to Enhance National and Multi-National Cooperation," *Information & Security: An International Journal* 3 (1999), 12-24.
2. For details the reader may refer to the article "National Military Command Center - From Idea to Implementation" by Nikolay Petrov in the current volume.
3. At the Brigade level, the C2 requirements and Systems must address both the planned Field Integrated Communication Information System (FICIS) Brigade and those Brigades not currently scheduled to have a FICIS capability. For details on FICIS refer to Stoyan Balabanov, "Field Integrated Communications and Information System for Bulgarian Land Forces," in this volume.
4. A similar requirement exists for the Air/Air Defense Forces and Naval Forces.

Dr. Daniel F. WIENER II and **Mr. John COURTIEN** are currently with BAE Systems North America, Communications Group. E-mail: john.courtien@baesystems.com

BACK TO TOP

Bulgarian Information Network: Command Information Infrastructure for the Future

Daniel F. Wiener II and John Courtien

Keywords: Defense Information infrastructure, C4ISR, mobile combat radio network, mobile IP network, information assurance, crisis management.

Abstract: The authors present a vision for the Bulgarian Information Network (BIN) that is globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to Government, warfighters, law enforcement, policy makers, and support personnel. The BIN includes all owned and leased communications and computing systems and services, software (including applications), data, security services and other associated services necessary to support mobile, Government information operations. The BIN connects the Government personnel to capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites) and provides interfaces to coalition, allied and coalition users and systems. BIN serves as backbone of the C4ISR defensive, crisis management and law enforcement operations.

full text

Author: **Nikolay Petrov**
Title: **National Military Command Center - From Idea to Implementation**
Year of issuance: **2001**
Issue: **Information & Security. Volume 6, 2001, pages 69-81**
Hard copy: **ISSN 1311-1493**

NATIONAL MILITARY COMMAND CENTER - FROM IDEA TO IMPLEMENTATION

Nikolay PETROV

Table Of Contents:

Introduction

The idea for National Military Command Center (NMCC) was derived in the course of C4 system studies, conducted in several Central and Eastern European countries by US Air Force Electronic System Center, Hanscom AFB, and MITRE Corporation.

A common thread emerged from the analysis of national C4 system requirements and on-going modernization plans. Basically, all nations, involved in the studies had the same problem. They were engaged in planning for the introduction of centralized information collection and processing systems to support the management of military forces in crisis situations. Because these systems were being planned independently, there was little commonality of system concepts or system architectures. Consequently, the ability to share information among nations in a regional crisis and to collaborate in crisis relief actions would, most likely, be severely limited.

In response to the apparent need for a centralized crisis management capability and in the spirit of the Regional Airspace Initiative, which resulted in an Air Sovereignty Operations Center (ASOC) program, the U.S. Air Force Electronic Systems Center (ESC) developed a concept for implementation of a *National Military Command Center* for crisis management. This command center, identified as the NMCC, would support both national civil and military crisis situations and, because different national systems would be built on a common architectural platform, it would also support regional collaboration in response to regional crisis situations. This NMCC concept was presented to several nations in the spring of 1999 and met with favorable response.

Based on this response, the U.S. government formally introduced the new policy initiative to Partnership for Peace nations at a multinational conference in Sofia, Bulgaria in June 1999. As described in the U.S. keynote address at the conference, the NMCC was intended to provide national command authorities with a modern, integrated command and control facility to support decision-making in the event of civil or military crises.

Further, the NMCC will be built on a NATO and US-compatible technical architecture and operational environment platform – NACSP (NATO Common Standard Profile), JTA (Joint Technical Architecture), COE (Common Operating Environment) – and will provide interfaces that are compatible with comparable NATO and U.S. command and control systems.[1]

At the conference seven countries indicated they would collaborate in the initiative, most as active participants. Since that time, several other countries have expressed interest in the initiative. The next step in the process of advancing the initiative was forming a multinational Working Group of potential program participants. The Work group had three meetings - in Predeal, Romania in September 1999, Piestany, Slovakia in March 2000 and Wroclaw, Poland in June 2000. Representatives of the Bulgarian Ministry of Defense (MoD) attended all meetings and presented the national point of view. The Working Group agreed and established a Concept of Operation (CONOPS) and Technical architecture framework for the NMCC. These two documents will serve as the foundation for an acquisition effort for all nations, choosing to participate in the NMCC project.

Vision

The NMCC is a secure, data integration, information processing, display and distribution command and control facility. It is intended to be used at the MoD - General Staff level to support senior national decision-makers in coordinating crisis management activities. The system will interface with national military Service Headquarters, with national military and civil information sources and with national civilian agencies and organizations involved with crisis management. As such, the NMCC is one part of the entire national crisis response mechanism. It may also be used to support regional coordination in the event of crisis situations that affect large regional areas. NMCC functional capabilities will include a core set of features common to all nations, thus promoting interoperability, and an optional set of additional functions tailored to unique operational requirements of the armed forces of each country.

General tasks for the NMCC are:

- To collect and correlate information on the scope and nature of a crisis. This includes situational information, status of forces and resource information.
- To provide means to consolidate information received from disparate sources into a comprehensive picture for decision support at the highest national level.
- To provide capability to coordinate crisis response activities with other national organizations involved in the crisis management process.
- To provide vehicle for collaboration with regional/coalition partners in cases where crises cross, or may cross national boundaries.
- To provide mechanism for communications and order dissemination to relief units.

The NMCC system hardware and software will comprise mainly commercial off-the-shelf (COTS) packages, augmented by government (GOTS) and coalition packages developed to support command and control applications.

Mission

A *crisis* can be defined as an incident or situation involving a threat to a country, its territories, citizens, military forces, possessions, or vital interests that develops rapidly and creates a condition of such diplomatic, economic, political, or military importance that commitment of national military forces and resources is contemplated to

achieve national objectives. It may occur at a local, provincial/county, national, or regional (international) level. A crisis may be natural or man-made. Examples of crises include: natural disasters (e.g., fires, floods, earthquakes, avalanches), terrorist activity, industrial accidents (e.g., nuclear reactor incident, hazardous material spill), pandemics, aggressive military acts of another country, mass immigration emergencies, civil unrest with acts of violence, and others.[2]

Republic of Bulgaria has laws and plans in place that define what can be done in times of crisis. Most disasters and emergencies are handled by the Civil Protection service, police, fire departments, emergency service, hospitals, and support agencies. The government is asked to provide additional assistance when the consequences of the crisis exceed the local and provincial/county capabilities. Various emergency teams, support personnel, specialized equipment, operating facilities, assistance programs, and access to private sector resources constitute the overall national crisis operations system. Types of assistance needed for crisis management include transportation, communications, public works and engineering, fire fighting, information and planning, resource support, health and medical services, search and rescue, hazardous materials handling, food, and energy. Organizations and agencies involved in the crisis operations include the government; ministries associated with transportation, agriculture, internal affairs, external affairs, defense, justice, etc.; Civil Protection Service; international relief organizations such as the Red Cross or coalition organizations such as the Euro-Atlantic Disaster Response Coordination Centre (EADRCC) of NATO; relief organizations and governments of other countries; private sector relief support; and others.[3] Crisis response actions are usually prioritized as follows:

1. First priority is always the safety of the emergency responders and the public.
2. Second priority is to provide stabilization of the crisis by minimizing the effect that the crisis may have on the surrounding area and maximizing the response effort while using resources efficiently.
3. Third priority is to minimize damage to property while achieving the crisis management objectives.

In addition to crises that affect national interests, Bulgaria also supports peacekeeping operations beyond national borders. Sometimes this may be within the region but sometimes an operation may be further away. Such support may consist of sending humanitarian aid, medical units, engineering units, transportation units, observers, etc. This support requires coordination not only among national agencies, but also international coordination.

Strategy

The NMCC will be a centralized facility to provide national-level coordinated management for military and civil crisis response. It will be controlled and operated by the General Staff, with civil agency participation/liaisons when necessary.

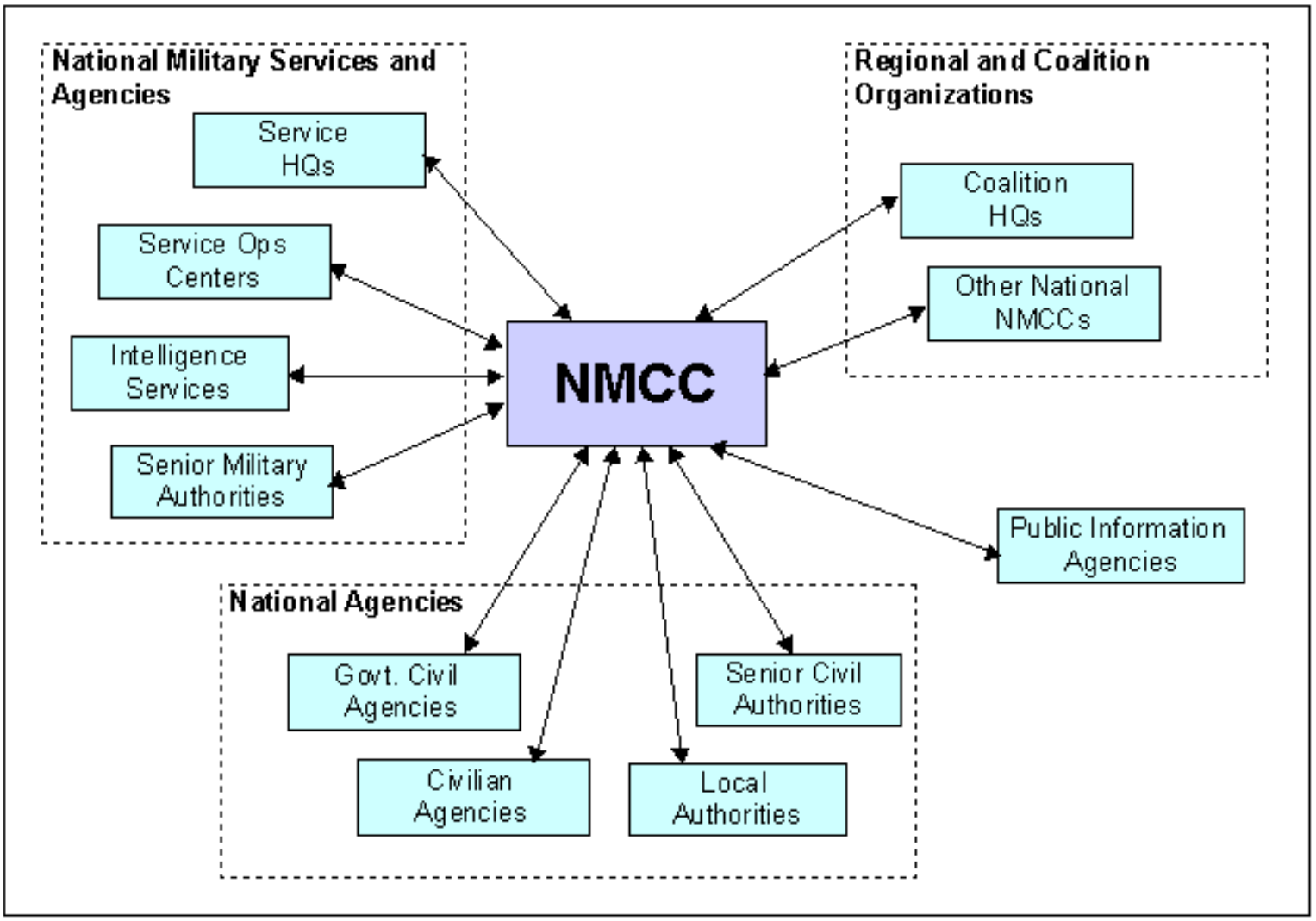


Figure 1: NMCC Operational Relationships

The NMCC uses interfaces with service headquarters, national military information sources, national civilian agencies/organizations, and regional or foreign agencies/organizations to receive and disseminate information.

The NMCC will be employed at the strategic level within the Bulgarian Armed Forces command and control structure.[4] It will operate on a 24-hour/7-day schedule. Normal staffing (pre-crisis) is minimal. In times of crisis, a Crisis Action Team (CAT) area will be set up and the staffing for the entire NMCC will be augmented as needed.

In support of crisis management activities, the primary functional capabilities of the NMCC are as follows: [5]

- *Situation Monitoring (information collection/retrieving).* Collection and correlation of information from military services, intelligence sources, civil sources, commercial news services, etc.
- *Situation Assessment (information processing).* Evaluation of Force capabilities, planning for resource application, use of mapping displays, access to national emergency planning information, etc.
- *Information Distribution.* Preparation and distribution of messages to organizations concerned with crisis management.
- *Report Generation.* Preparation of reports and briefings for senior national authorities and also for use in regional cooperative activities, as well as for coalition authorities (if appropriate).

- *Database Management.* Generation of and updating databases that are important to crisis management activities. Examples include databases for Logistics, National Infrastructure, Personnel and Medical.

  Information will be received, processed, distributed and protected generally by following services: [6]

  - Clear and secure voice;
  - Clear and secure email (SMTP/POP 3, X.400);
  - Clear and secure fax;
  - Clear and secure messaging - unformatted and formatted (USMTF, ADatP3);
  - Data link (Link 1, Asterix);
  - Clear and secure internet/intranet (TCP/IP based LAN/WANs);
  - Audio/visual source (e.g., radio, television, VTC - H.320 or IP-based);
  - Common Operational Picture/Geographic Information System (COP/GIS) functions
  - Computer Aided exercises/Modeling and Simulations (CAX/M&S) functions;
  - Computer Based Training (CBT) / Online Training / Online Help functions;
  - Data Management services;
  - Firewall equipment and services;
  - Guard equipment and services;
  - Communications Security (COMSEC) equipment and services;
  - Selected gateways;
  - Anti-virus software;
  - National standards and policy based security key management;
  - Printed materials, etc.

In addition, the system may have remote monitors or alarm systems located in the NMCC for disseminating radiation and seismic information.

Through the use of a messaging system and a data link translator, the NMCC will have the capability to automatically process some of the digital data and store it in databases for analysis and presentation. Other information will require operator input or intervention (e.g., manual entry, cutting and pasting, file saving using office automation, database and email capabilities) for adding to the NMCC databases to be displayed later in a graphical or text format.

Operations within the NMCC can be separated into four periods, associated with crisis management: pre-crisis, situation development, crisis response and recovery, and post-crisis.[7]

Pre-crisis operations

Pre-crisis operations are performed when no crisis or potential crisis has been identified. Staffing is minimal

and normally occupies the Operations Center. This is often called the "watch-keeping" effort and the NMCC is often called at this point a "Situation Center".

During pre-crisis operations the following functions are performed:

- Situation monitoring: The NMCC staff will maintain up-to-date situation information using mainly public information sources (e.g., news and weather) and military and national agency sources. This information will include items such as:
    - current and predicted weather;
    - current events in-country and within the region, e.g., political, social and/or economic activities/ problems/ trends;
    - planned activities and resource status reports/updates from the Services and other military or civilian agencies and organizations;
    - updates for national and international level shared data such as resource information (equipment, personnel, etc.), joint contingency plans (e.g., plans involving more than one agency, organization, or nation); [8]
    - updates to relevant reference information (e.g., national plans and policies; mapping data such as updated political boundaries, areas of responsibilities, flood plain information, evacuation routes, communications and transportation infrastructures, population densities, fixed support facilities such as potential shelters, hospitals, police/firefighting units, etc.);
    - Intelligence information.
- Situation assessment: The NMCC staff will assess the available information to determine the possibility of potential crises. They will use the NMCC's Geographical Information System (GIS) capabilities to view a consolidated situational display Common Operational Picture that fuses situational data from air, land and naval forces) with associated mapping information. The NMCC staff will use links from the Common Operational Picture, as well as database queries and generated reports to analyze database information such as resource status and availability.
- Status reporting: The NMCC staff will provide daily status reports to Service headquarters and national agencies. This will be done using NMCC graphical and textual report generation capabilities and transmitted via voice or data communications, printed format, or formal briefing. Video teleconferencing (VTC) will be used to disseminate this information to selected facilities.

In addition to the above daily functions, the NMCC may support the following:

- Operator training: Workstations for augmentation personnel may be used for operational training purposes during pre-crisis operations.
- Exercises: The NMCC may be asked to participate in national or regional/coalition exercises. The NMCC would then be required to handle both real and exercise information.

Situation development operations

Situation development operations are performed when the potential for a crisis or an actual crisis has been

identified. The minimal staffing is augmented as the situation escalates. The following functions are performed:

- Situation monitoring: The NMCC staff will continue to maintain up-to-date situation information using military, national, and public information sources. As a situation develops, the NMCC staff will focus *on gathering timely detailed information pertinent to the situation.* This information will include items such as:
    - current and predicted weather (e.g., flood warnings or heavy rains in low-lying areas);
    - current events in-country and within the region;
    - planned activities, resource status reports/updates, and *alerts and warnings;*
    - from the Services and other military or civilian agencies and organizations;
    - updates for shared data such as resource information and joint contingency plans;
    - updates to relevant reference information;
    - intelligence information;
- Situation assessment: NMCC staff will assess the situation information to determine the nature and possibility of potential crises using the following tools:
    - GIS tools, supporting the Common Operation Picture (COP).
    - Links from the COP and database tools (e.g., queries, reports). The NMCC staff will identify major constraints (e.g., severe weather, potential breakdown of communications, power or transportation infrastructure, political consequences, etc.).
    - Office automation tools will be used to access NMCC plans and procedures that the NMCC staff will follow as the situation escalates, as well as existing contingency plans and Courses of Action (COAs) that may be used in managing the crisis.
- Coordination: As the situation develops, the NMCC staff will begin coordinating with the Service Headquarters and other national agencies and organizations to request, gather and share information. The NMCC staff will start to coordinate with other nations in the region if the situation could impact areas beyond national borders. Data sharing will include mapping information, resource status, operational plans, etc., using the mechanisms identified in the situation-monitoring paragraph above. Video Teleconferences (VTCs) will be used for the real-time exchange of information with selected facilities. Collaborative tools will also be used for the real-time sharing and modification of information and documentation.
- Notification: NMCC staff will notify senior authorities of a potential or existing crisis normally via voice communications. Senior leadership will officially declare the crisis.
- Status reporting: NMCC staff will provide status reports to Service headquarters and national agencies. This will be done using NMCC graphical and textual report generation capabilities. The reports can be transmitted via voice or data communications, printed format, or formal briefing. VTCs will be used for selected facilities.

Crisis operations

Crisis operations are performed once a crisis has been officially declared and until MoD support to the specific

crisis has ended. The first step in this period is the creation of a Crisis Action Team(s) - CAT in response to the official crisis declaration and the NMCC staffing is augmented accordingly. Augmentation staff from the previous period (Situation Development) will support the Operations Center or the CAT. All rooms in the NMCC are used. The following functions are performed in the NMCC during crisis operations:

- Crisis monitoring: The NMCC staff will continue to maintain up-to-date situation information using all sources available. Information will be focused on results of field activities.
- Crisis assessment: NMCC staff will continue to assess the situation information to determine the nature and scope of the crisis using the following tools:
    - GIS tools, supporting the Common Operation Picture (COP), will be used to display a consolidated recognized situational picture.
    - Links from the COP and database tools will be used to access and correlate stored information. Some of this information will be stored locally; the NMCC will also have access to other national emergency information managed by other agencies. Using resource status information, NMCC staff will evaluate the nation's continuing capability to respond to the crisis, e.g., what resources (land, maritime, air forces; civilian resources) are needed to respond to the crisis, are they located where they can respond or must they be moved, do they have the resources operational and available to support the crisis, etc.). The NMCC staff will identify major constraints, e.g., severe weather, potential breakdown of communications, power or transportation infrastructure, political consequences, etc.
- Planning: NMCC staff will establish command relationships with the service HQs, based on the nature of the crisis (e.g., a crisis on the Black Sea will require Navy involvement). They will use office automation tools to access NMCC plans and procedures that the NMCC staff will follow as the situation escalates, as well as existing contingency plans and COAs that may be used in managing the crisis. They will review the existing plans and COAs for applicability and recommend additions or modifications to the MoD/General Staff.
- Execution: The NMCC staff will disseminate operational decisions taken by the MoD/General Staff and then monitor the execution of the decisions and the resulting deployment and employment of forces. Through coordination with the various agencies and organizations, the NMCC will identify conflicts or issues and will recommend COAs to the MoD/General Staff for their resolution.
- Coordination: As the crisis evolves, the NMCC staff will continue to coordinate with the Service HQs and other national agencies and organizations to request, gather and share information. The NMCC staff coordinates with other nations in the region, or area of interest, if the situation impacts areas beyond national borders (e.g., flooding, nuclear incidents, peacekeeping activities). Data sharing will include mapping information, resource status, operational plans and status, potential conflicts with resource management/logistics, etc., using the mechanisms identified in the crisis-monitoring paragraph above. VTCs will be used for the real-time exchange of information with selected facilities. Collaborative tools will also be used for the real-time sharing and modification of information and documentation.
- Status reporting: NMCC staff will provide status reports to Service headquarters, national agencies and senior national authorities and also for use in regional cooperative activities and for coalition authorities (if appropriate). This will be done using NMCC graphical and textual report generation capabilities and transmitted via voice or data communications, printed format, or formal briefing. News media will be notified to inform the public of on-going plans/actions and support available.

Post-crisis operations

Post-crisis operations are performed once MoD support to a specific crisis has ceased. Staffing is reduced eventually to the minimal "watch-keeping" level. Post-crisis operations are conducted concurrently with the pre-crisis operations. The following functions are performed:

- After-action reporting/analysis: The NMCC staff will reduce compiled data and analyze operations conducted to identify lessons learned and support future plans and operations. Using databases and office automation tools they will generate after-action reports and will modify existing plans based on the lessons learned. NMCC staff will coordinate lessons learned and changes to joint planning documents with other organizations and agencies, and other nations (if appropriate) that supported the crisis management effort. This will be done through meetings, VTCs, email exchange, and/or collaborative tools.
- Stand-down: NMCC staff will notify military and national agencies of the cessation of military support. News media will be notified to inform the public of these actions. The NMCC will also coordinate with regional/coalition partners, if appropriate, in the termination of the crisis management support.

The NMCC cannot function alone. It is only one element of a national crisis response capability. The NMCC relies on national information sources and, in turn, provides correlated and processed information to national military and civil organizations and agencies. Furthermore, the NMCC may play an important role in regional crisis management activities. It may be used to support national participation in coalition operations, including NATO operations.

NMCC is not intended to replace existing or planned national crisis management system or command center. Instead, the NMCC is planned to complement and to enhance national crisis management capabilities. As such, the NMCC will be integrated in national C2 system with other national crisis management systems to the maximum extent practical. This requires establishing interfaces between the NMCC and a number of national and regional organizations and systems. These interfaces are identified generically as:

- National Military Service HQs;
- National Military Information Systems;
- National Agencies and Systems;
- Public Information Agencies and Systems;
- Regional and Coalition Organizations;
- Deployed NMCC Capability;
- Senior Leadership Communications Capability.

In general, these interface categories are optional and implementation will be an object of national decision.

NMCC is a high priority project for the Bulgarian MoD. It is important part of the overall process of C4 study recommendation implementation and is also a program element of MoD's Main program 10 "C4ISR systems modernization." [9] The project will be funded by US Government FMF funds for Bulgaria (2001) and by MoD budget funds. According to approved schedule, NMCC is expected to be operational in the end of 2002.

Notes:

1. Roland J. Roland, "Applying modeling and simulations to enhance national and multi-national cooperation", *Information and Security: An International Journal* 3 (1999), 12-24.
2. *National Military Command Center Concept of Operations (CONOPS)*, Working Document (18 August 2000).
3. Velizar Shalamanov and Todor Tagarev, *Information Aspects of Security* (Sofia: Procon, 1996).
4. See *Command, Control, Communications and Computers Study for Bulgaria* (Hanscom AFB, MA: Electronic Systems Center/MITRE, 2000).
5. Neil Planzer, "Regional Airspace Initiatives in Eastern Europe," *ATC Quarterly* 2 (April- June 2000): pp. 11-16.
6. *National Military Command Center Technical Architecture Description* (21 August 2000).
7. *National Military Command Center CONOPS.*
8. Velizar Shalamanov and Todor Tagarev, "Object Oriented Model to Support Early Warning and Rapid Reaction Planning in International Context." in *IFAC Conference on Supplemental Ways for Improving International Stability SWIIS'98* (Bucharest: IFAC, 14-16 May 1998), pp. 47-52.
9. Velizar Shalamanov, ed., *Cornerstones of Bulgarian Security and Defence Policy* (Sofia: Ministry of Defence, July 2001).

Lieutenant Colonel **NIKOLAY PETROV** is Head of C4ISR section in the “Armaments Policy Directorate” of the Bulgarian Ministry of Defense. He was promoted to this position after serving as Senior Expert in the “Programs for Development of Armaments, Equipment, and Infrastructure” section of the Defense Planning Directorate in the Ministry of Defense. He was born January 1st, 1959 in Montana, Bulgaria. LTC Petrov graduated Technical University in Sofia in 1982. He has a M.Sc. Degree in Computer Automation of Industry. He served as a Chief of section "Automation" in Central Command Post of Bulgarian Air Force until 1990 and as Chief of section "Systems" in Air Force HQ Computer Center until 1998. He graduated USAF BCOT course in Keesler Air Force Base in 1998.

BACK TO TOP

National Military Command Center - From Idea to Implementation

Nikolay Petrov

Keywords: NMCC, CONOPS, technical architecture framework, crisis, pre-crisis operations, situation development operations, crisis operations, and post-crisis operations.

Abstract: This article addresses issues related to the creation of a National Military Command Center (NMCC). It gives the background of how the idea of NMCC emerged and how it developed, namely the creation of a multinational Working Group of potential participants in the project, the Concept of Operation (CONOPS) and the Technical architecture framework for the NMCC. It also discusses the general tasks, which the NMCC is going to perform as well as its functional capabilities and operations..

full text

Author: **Stoyan Balabanov**
Title: **Field Integrated Communications and Information System for Bulgarian Land Forces**
Year of issuance: **2001**
Issue: **Information & Security. Volume 6, 2001, pages 82-93**
Hard copy: **ISSN 1311-1493**

FIELD INTEGRATED COMMUNICATIONS AND INFORMATION SYSTEM FOR BULGARIAN LAND FORCES

Stoyan BALABANOV

Table Of Contents:

Introduction

The development of command, control, communications and information systems is a priority in the development of the Bulgarian armed forces, established in the Governmental Program for NATO Accession [1] and confirmed by Parliament with the adoption of the Military Doctrine of Republic of Bulgaria.[2] In implementation of the declared priorities, the first major modernization project was for development of the field communications and information system of the main land formations of the Bulgarian rapid reaction forces, that would contribute to NATO and NATO-led peace support operations. The tender for the project, that became known as the FICIS (Field Integrated Communications and Information System) project was conducted in 1998. During its implementation requirements were influenced by the knowledge and experience gained by military leaders and experts during the comprehensive C4 Study,[3] as well as by dedicated seminars and discussions.[4]

The FICIS system has to provide NATO interoperability through advanced C2 capability of one mechanized brigade, one engineer battalion, one battalion for NBC defense, and one company for radiological and chemical surveillance. This article presents architectural requirements of the Bulgarian Land Forces that will be met by the FICIS System. Starting from an in-depth analysis of

general requirements stated in the Technical Annex to FICIS Contract, the overall architecture of the system is developed and, at the same time, optimized to guarantee efficiency and flexibility. The article covers five main issues. First, we explain the technical reasons behind the contract negotiations in terms of number of telecommunication vehicles (stations), equipment, software packages and services. Secondly, clarifies the ways for connecting stations and their interfaces. The third part contains an example of Brigade deployment on the field. The fourth part of the article contains a brief explanation of software and hardware devices for configuring and managing the network and the services. Finally, clarifies how the Command and Control applications work through the FICIS network.

1. Initial Requirements - Project Milestones

In this section, technical reasons behind FICIS architecture are briefly explained. The project milestones are listed with a brief explanation of the agreed solution.

Radio Access Points (RAP)

There are a total of four Radio Access Points in the system. This choice was made under both technical and operational considerations:

- When operating in stand-alone configuration, the brigade, the Combat Engineer Battalion (CEB), the Nuclear, Biological and Chemical Defense and Radiological Battalion (NBCDRB) and the Radiological and Chemical Surveillance Company (RCSC) can be assigned one RAP each, to support fixed to mobile and mobile to mobile communications needs. More than one RAP could be assigned to any mission (e.g. four RAPs can be assigned to the brigade);
- The necessity of having at brigade level more RAPs to support close-to-FEBA (Forward Edge Battle Area) operations has been partially reduced by providing the three mechanized battalions and the anti-tank battalion with a Mobile Command Post (MCP) equipped with a Light of Sight (LOS) radio relay to support multi-channel communications towards the brigade command post. It has been in fact recognized that connections with the battalions' subordinate units (companies, platoons, etc.) are established up to the battalions' commander, thus removing the need of direct Combat Net Radio Access (CNRA) connections to the brigade headquarter;
- .RAPs can indeed be used to increase the distance between the battalions' command posts (CPs) and the brigade CPs; in this case the Mobile Command Posts (MCPs) and Main Mobile Command Post (MMCP) represent the mobile users to the RAPs. This concept is applied throughout the system and at any command level;
- Each RAP supports three VHF radios and one HF radio; based on the data provided by HARRIS and considering the IP data application, each RAP can satisfactorily support up to 75 VHF mobile users and 25 HF users. This leads to a total capacity of up to 300 VHF Mobile Units (MUs) and 100 HF MUs. In the case of voice connections, the figures are not greatly affected if the average duration of a call is less than 30 seconds;
- Considering any one MCP/MMCP in the brigade as a potential MU to a RAP, and considering

that only one VHF and one HF radios will be used to RAP affiliation, then the overall MCP/MMCP contribution equals to 46 VHF MUs;

- As for the sub-units, the overall number of radios is 456 VHF (excluding handheld radios) and only 32 HF vehicular or man-pack radios. It must be considered that only part of the CNR (Combat Net Radio) radios will be affiliated to the RAPs during real operations (due to user dispersion), or even that not all of them could be used at the same time (due to the resulting frequencies congestion that does not depend on RAP implementation).
- In conclusion, the number of RAPs (four) appeared to be adequate to the extension of the population to be served, to the traffic to be supported and even over-sized as for the HF application. It is recognized that the system can be scaled to population and traffic demand increase.

The Access Vehicles (AV)

The total number of Access Vehicles assigned to the Brigade depends on the requirement to provide Brigade Command Posts and Battalions' Command Posts with a WAN access point each.

Further two AV* (Access Vehicles or Extended Access Vehicles) are assigned to Main and Logistics Command Posts; also CEB, NBCDRB and RCSC Applications are provided with AVs.

The Transit Access Vehicles (TAV)

Only two TAVs are included in FICIS; both are assigned to the brigade.

Deployment of Single Channel Radios

A total of three VHF and one HF radios per RAP/MMCP and MCP are deployed to minimize mutual interference problems and to maximize the bandwidth exploitation.

Four mobile 400W HF systems are provided - one per application.

2. Interfaces

Many interfaces are used in the FICIS system in order to provide a complete, efficient, secure, and versatile network equipped with diverse applications and services.

Radio Relays

Two types of radio relay are used:

- MH313/X: Eurocom standard radio relay, band III extended (1350-2700 MHz), 2048 Kbit/s data rate;
- MH344: Eurocom standard radio relay, band IV (4400-5000 MHz), 2048 Kbit/s data rate.

Installed in Backbone Access Vehicles, these types of equipment guarantee meshed connections among FICIS digital switches (CD115E); such connections are made secure by using CM119 Bulk Encryption Devices.

Wired connections

Installing MT323/D Line Terminating Unit (LTU) inside Access Vehicles provides wired connections among stations. There are two types of channels:

- STANAG 4210 up to 512 Kbit/s;
- Eurocom C: up to 2048 Kbit/s.

As Radio Relays, also LTU are also used to provide connections among digital switches.

Single Channel Radios

Harris Falcon II VHF and HF radios aim to guarantee both connections between Backbone Command Posts and Subordinate Units (Sub-Units) Mobile Vehicles, and links among Sub-Units themselves.

- VHF: up to 16 Kbit/s for both voice and data, DTE channel for voice and Ethernet 10Base-2 for signaling and data in TCP/IP format;
- HF: up to 2.4 Kbit/s (600 bit/s hopping) for both voice and data, DTE channel for voice and Ethernet 10Base-2 for signaling and data in TCP/IP format.

CNR voice function is implemented through DTE channel connecting CD115E radio interface (DGTRAD board put into RAP vehicles).

CNR signaling is hosted by Ethernet interface directly passing through the Hub-Switch (included in RAP vehicles).

TCP/IP function in the radios is made by embedded hardware and software, so that the radios are directly connected to the Ethernet 10Base-2 line.

MMCP and MCP with Radio Relay vehicles, their digital switches CD115 being not equipped with DGTRAD board, cannot work as a "gateway" for voice CNR function, but they can also route TCP/IP packets thanks to routers installed in such vehicles.

Optical Link

Fiber Optic links are used to connect Hub-Switch, contained in vehicles, in chain way in order to make physical LANs working apart from the system, without taking resources from the WAN network.

This solution can improve system performance in two ways:

- By connecting many vehicles thus establishing high performance LANs (100 Mbit/s); this LANs will be homogeneous in terms of functions, operations, deployment, military hierarchy;
- By reducing traffic on WAN system, because LAN traffic is not routed through WAN if not strictly necessary. Only effective remote connection is to be made through the WAN.

External Interfaces

A pool interfaces to other networks is implemented in the FICIS System, at Access Vehicles (through Digital Switches).

- Eurocom "c" trunks with 16 channels at 16/32 Kbit/s according to the standard (256 and 512 Kbit/s)
- STANAG 5040 multi-channel analogue gateways
- STANAG 4206-4210 digital multi-channel gateway
- ISDN ETSI interfaces at 144 KBit/s (BRI to ISDN terminals)
- ISDN ETSI interfaces at 2048 Kbit/s (PRI)
- Analogue 2/6 wires analogue circuits to PTT networks or PABXs.

3. System Network Architecture

Different links are used depending on deployment requirements:

- Meshed Backbone
- Multi-channel radio links
- Optical links
- Wired connections
- Combat Net Radio networks

Also, Radio Access Point stations and Transit Access Vehicles are deployed.

4. Network Management

Since the FICIS System has a very complex architecture with different equipment and services, many network management packages are needed to cover all aspects.

Marconi NMS (Supervisory System)

At telecommunication equipment level, operations, network and equipment management is guaranteed by Marconi Supervisory System that applies to three different levels working together in a synchronized way:

- System Execution and Planning;
- Operational System Control;
- Facility Control.

The three levels can manage the entire telecommunication network from highest level, i.e., brigade deployment requirements, down to lowest physical detail, i.e., a specific board in any equipment.

The three levels run under SCO Unix operating system, on a dedicated computer family. Connections between supervisory nodes are established through the WAN system by means of gateway function realized by the general block identified as "Gateway".

This functional block represents CD115 Digital Switch and ATI-3100 Router joint functions.

The Routers route TCP/IP data trough digital switches that guarantee a meshed network.

Mapping this architecture with the brigade deployment, the two SEP (System Equipment Planning) posts are placed in the brigade Main and Logistics Commands. The OSC (Operational System Control) post is placed at the brigade’s Deputy Command; in each telecommunication vehicle is placed a FC (Facility Control) post.

A Telephone Numbering Plan will be prepared and submitted to the user for discussion and approval.

NMS Operative Flow

The system can accept and manage maps in different formats. The system can manage encryption keys in conjunction with the KS119 Key Generation System included in FICIS.

System Execution and Planning

The SEP Rear post is aligned with the Main in order to be easily promoted to Main, when needed. The SEP level directly exchanges information with the OSC level.

Operational System Control

The OSC level directly exchanges information with both upper SEP and lower FC levels.

Facility Control

The FC level directly exchanges information with upper OSC level.

Microsoft NT^{TM} Administration and Management

At information subsystem level (computers and peripherals), network administration is demanded to Microsoft NT^{TM} administrative tools. Many services will be enabled in the system in order to facilitate and to make automatic complex and boring activities.

Primary/Backup Domain Controllers and Resource Servers will be placed in the system in such a way to guarantee best performance and balanced use of communication channels (WAN system).

User Account will be managed under in respect to Microsoft constraints; management will be open for all relevant aspects as groups, permissions, rights, sharing resources, priority.

DNS and WINS services will be enabled to automatically resolve IP addresses from computer names.

DHCP service will be enabled to allow centralized automatic management from the brigade Main Command.

A *Private Network IP addressing model* will be adopted to make the network flexible and to guarantee coverage of necessary devices. An IP addressing plan will be created and submitted to the user for discussion and approval.

A specific software package [5] is to be adopted for easy monitoring of network status, in centralized manner.

Five Firewalls, included in FICIS (two assigned to the brigade Main and Logistic CPs, one for CEB, one for NBCDRB and one for RCSC), will be set up in *Bastion Host* configuration, for better protection of secure access from/to outside FICIS, allowing flexible and centralized monitoring and configuration.

Routing Techniques and Router Administration

Routers' configuration and monitoring can be made in two ways.

- At power-on, routers will start in a brigade standard (pre-defined) configuration option, that will allow each router to be basically connected to the WAN system through local digital switch; then a centralized operator (i.e., at SEP level) can modify configuration of each router to accomplish mission specific requirements;
- At start-up, also predefined routing algorithms will be loaded automatically by routers to establish the meshed network.

Some static routes will be put (manually or automatically) for defining into routers the right paths for linking Mobile Users.

Single Channel Radios Administration

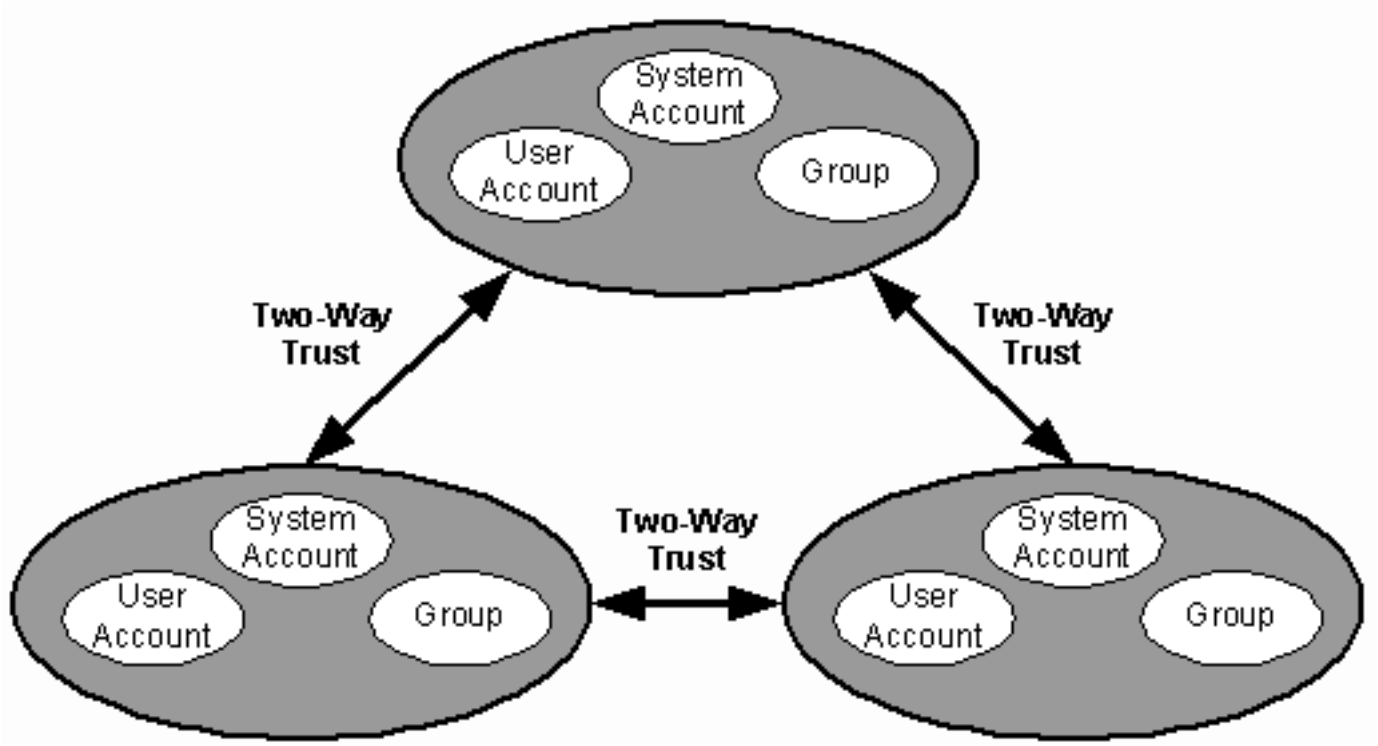
VHF and HF Radios will be configured by means of VHF and HF Network Management Software, that is Harris Radio Programming Application™ software package (RPA). Each radio will be defined as a "net member" using RAP. Then the operator will upload each radio with proper configuration file.

The RAP software runs on CNRA Station and flows over Ethernet.

5. Command and Control Architecture

Operating system

The operating system for the Command and Control will be Windows NT. There is no strict relation between NT Server and Command and Control Servers or between NT Workstation and Command and Control Workstations. The Model for the definition of Windows NT domain is named *Complete Trust Model* shown in following figure.[6]



Database Management System

The Database Software Package for the RDBMS is ORACLE; the data model will be the Generic Hub 3.

The Data Base architecture is based on the following principles:

- Each CP LAN has its own "copy" of the Operational Database, resident on the CP server that

stores all the information about the RLP (recognized land pictures).

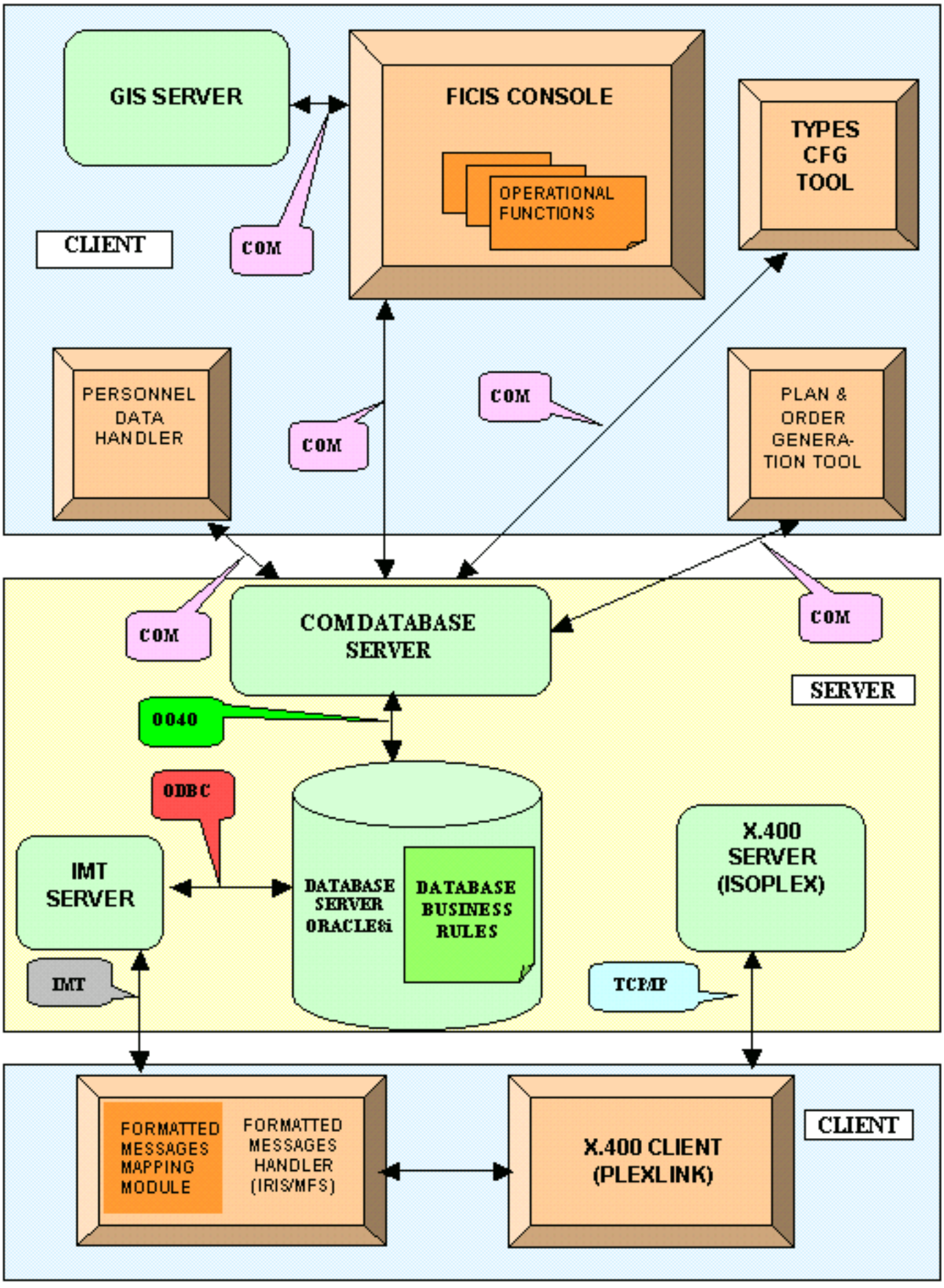
- All databases share the same data model (based on the ATCCIS GH3 data model).
- Each workstation has its own local working area (private DB) to perform its activities (plan preparations, line of action evaluations, etc.)
- A replication mechanism ensures that the Database of all the CPs are maintained aligned on transaction basis.
- The replication mechanism takes care, in case of network failure between two nodes, to store transactions.
- The replication mechanism will maintain aligned the CPs' Databases, if they are connected by a LAN or by a WAN provided by sole users' circuits.
- The replication mechanism will maintain aligned the CPs' Databases on user request, if they are connected by a WAN provided by radio channels.
- The software package for the data management will be the Oracle Administrating Tool.
- The role management functions will be provided by a software package delivered by Marconi.

Geographic Information System (GIS)

ESRI Map Objects and ESRI Arc/View compose the software platform for GIS applications (with the extension of "Spatial Analyst" and "Network Analyst" in the workstation).

- Map Objects will be used for the core application (FICIS Console) that will provide the user the basic GIS functions.
- Arc/View and its extensions will be used for the enhanced GIS functions, it will work in addition with the application based on Map Objects.

The *FICIS Console* is the main CCIS (Command & Control Information System) application (see the figure above). FICIS Console is the starting point for each specialized function, for example NBCDRB, Logistics, Office & Multimedia, GIS enhanced functions and so on.



Message handling System

The software package for the Message Handling System is ISOCOR ISOPLEX; each server CP will have an ISOCOR X.400 MTA; each workstation will be connected to the X.400 MTA server through the User Agent software.

Each User Agent will provide the client workstation the following capabilities:

- Send/Receive e-mail using the COTS ISOCOR PLEXLINK;
- Send/Receive formatted AdatP-3 messages using the COTS ISOCOR PLEXLINK in conjunction with the COTS IRIS/MFS.

Office Automation

The COTS for the Office Automation are the following:

- Microsoft Office Professional;
- Apple Quick Time 3 pro for Windows NT;
- Corel Photo Paint 8.

They will be provided on node basis.

Conclusion

FICIS Project is expecting to be deployed in the Land Forces in April – May 2002. During the 18-month warranty period the system shall be observed very precisely. According the results from this period the engineers will to trace out the best feature use of the System and the ways for its exploitation and improvement. The combat effectiveness of the units using FICIS has to be evaluated and compared with others that do not use digital Communications and Command & Control Systems. Such kind of independent assessment can be done if the units using FICIS take part in NATO exercises or in combined military formations and operations.

Notes:

1. *National Program for NATO Accession* (Sofia: Council of Ministers of the Republic of Bulgaria, February 1997).
2. *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.
3. *C4I Study for Bulgaria: Final Report* (USAF ESC/MITRE, January 2000); *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).

4. The readers may refer to Loren Diedrichsen, “Command & Control: Operational Requirements and System Implementation,” *Information & Security. An International Journal* 5 (2000), 23-40; Charles R. Myer, “C4ISR Architectural Frameworks in Coalition Environments,” *Information & Security. An International Journal* 5 (2000), 60-72.
5. Hyena by Adkins Resources.
6. *FICIS Project. System Design & Operational Guidelines* (October 2000).

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. Prof. Balabanov is project manager for the FICIS (Field Integrated Communications and Information System) project for rapid reaction units of the Bulgarian Land Forces. *E-mail*: sbalabanov@md.government.bg.

BACK TO TOP

Field Integrated Communications and Information System for Bulgarian Land Forces

Stoyan Balabanov

Keywords: C2IS, Tactical Communications Network, Radio Access Points, Mobile Command Post, Network Management System, Marconi NMS.

Abstract: The main technical and system features of the first entirely digitized brigade for the Bulgarian Land Forces are analyzed. Field Integrated Communications and Information Systems (FICIS) is EUROCOM D/1 based tactical telecommunications network. The Command and Control Information System (C2IS) is based entirely on the NATO's ATCCIS Data model.

full text

Author: **Peter Petrov**
Title: **Towards Creation of a Unified Information System of the Navies of the Black Sea Countries**
Year of issuance: **2001**
Issue: **Information & Security. Volume 6, 2001, pages 94-101**
Hard copy: **ISSN 1311-1493**

TOWARDS CREATION OF A UNIFIED INFORMATION SYSTEM OF THE NAVIES OF THE BLACK SEA COUNTRIES[1]

Peter PETROV

Table Of Contents:

Security environment and non-traditional challenges

The particular geostrategic position of the Black Sea in the transeuropean lines of communications and the national systems of transport, the availability of certain stocks of fish, petrol, gas and other natural resources determine the set of factors and often controversial interests exerting strong influence not only on sea navigation, but also on the security of the whole region.

External political factors

During the last years, external political factors have a prevailingly positive effect on strengthening the common security in the region. Although slowly, the confrontation model of international relations is replaced by a new model characterized my mutual cooperation that includes organization of future mutual activities. Inseparable parts of this model are the activities aimed at the organization and control of the navigation in the region. Main components of this regime are:

- Control over maritime traffic and economic activities at sea;
- Safety of navigation;

- Seamless functioning of the traffic control infrastructure;
- Rescuing human life at sea;
- Protection of maritime environment;
- Prevention of breaks of law and law enforcement, etc.

Economic factors

In terms of economics, we anticipate increase of the importance of the Black Sea and the Danube river transport communications as an important economic connection between East and West, resulting in significant economic profits. The consequent increased intensity and liberalization of the navigational regime evoke risks such as accidents on ships carrying various types of cargo, including hazardous ones, environmental pollution and ecological disasters, loss of human life, etc. The considerable increase in smuggling, drug trafficking, illegal traffic of arms and people is also expected. All these reasons make the functioning of the respective state authorities significantly more difficult.

Military factors

Instead of having destabilizing role as in the recent past, the military factor was transformed into an essential guarantee for the security of the Black Sea region. Traditions determine the special role of the national Navies in the maritime areas of the region. Having functioning infrastructure and experience in coordination of various activities, Navies are leading institutions in regional security cooperation.

During the past few years, the relations among the Black Sea countries, and respectively among their Navies, register continuous progress. Annual multinational naval exercises, the constant exchange of delegations, and the exchange of information on various topics became routine.

Potentially, this cooperation can be additionally activated through the search of cooperative solutions of common problems, such as:

- Protection of the interests of the Black Sea countries in their respective and agreed maritime territories;
- Strengthening the control of navigation;
- Conduct of combined operations for rescue of human life, ships and aircraft in distress at sea;
- Countering smuggling and illegal traffic of people, drugs and arms at sea;
- Control of maritime environment protection and elimination of the consequences of oil spillages, industrial and other ecological hazards;
- Coordination of combined activities at sea.

The accomplishment and the effective management of these activities promote the necessity to set up

a common system for control of navigation, exchange of information and data, and for combined management of crisis response, as well as for creation of a common database.

Organization of shipping by the Bulgarian Black Sea coast

Before discussing potential cooperation, let me briefly explain the organization of control of shipping by the Bulgarian Black Sea coast. At the present stage, on the Bulgarian Black Sea coast there are two independent stationary systems for surveillance, control of navigation and maritime boundary control. The first one is operated by the Bulgarian Navy, and the second one – by the National Service "Border Police." Both systems include coastal visual and radar surveillance sites and traffic control stations. Currently, there is no specialized shipborne or airborne surveillance capability included. The systems work in parallel, periodically exchanging—at certain levels—information of various matters of mutual interest. Both systems interact also with the following organizations:

- State Marine Administration;
- General Bureau "Customs";
- The port of Varna;
- The port of Bourgas.

The organization is influenced by ongoing reforms in a number of sectors.[2] Of particular importance is the demilitarization of the structures of the Ministry of the Interior, including the Border Guards Service – now Border Police, and the Ministry of Transportation.[3] This necessitates urgent organizational arrangements and technical measures to solve the following problems:

1. Positioning of radar sites along the coast does not provide for full control of shipping;

2. The variety of radar and communications equipment hinders compatibility, and even interoperability among the units of the system;

3. The low level of automation in information processing and information exchange impedes adequate decision making, especially in rapidly changing situations.

To overcome these problems we plan to design and build up a unified automated system for control of shipping. We call this system "Ekran" [4]

The vision of the Bulgarian Navy calls for the creation of a *national, automated radar system for control of navigation and protection of the sea borders*.

Ekran

The system is intended to provide data and information necessary for the control of shipping in the littoral zone, straits, and channels, for protection of the sea borders, environmental protection, rendering assistance to vessels in distress, rescue of human life at sea, countering contraband and

illegal traffic of drugs, people and arms at sea. The “Ekran” system will provide common operational picture, while the situation will be recorded and documented at control stations.

The system has to fulfill the following main tasks:

- Search, detection, identification, classification and tracking of surface objects (contacts);
- Automatic transmission of contact data and complete radar picture from every radar site to the control station;
- Automatic data processing, picture compilation and integrated display on digital maritime charts in a unified standardized coordinate system;
- Control and support of navigation in the littoral zone, straits, and channels;
- Support of rescuing human life, Search and Rescue (SAR) of vessels and aircraft in distress at sea;
- Documentation of surveillance data;
- Data transmission to the automated command and control system of the Navy, the State Maritime Administration, General Bureau “Customs,” ports, etc.;
- Automatic transfer of data and picture from aircraft and ship-based surveillance radars;
- Real time data processing for up to 200 contacts;
- Compilation of radar and digital chart display;
- Initiation of security zones, borders, channels, navigation limits and marks, etc.;
- Connection to the surveillance system of the Air Traffic Control authorities.

The “Ekran” system will have the following structure and composition:

- 12-15 independent unmanned radar sites positioned from Dourankulak in the North to Rezovo in the South, to provide high density of surveillance. They will be organized in two areas – northern and southern;
- 4-6 control stations for each area: one for the Navy, for the National Service “Border Police,” for the State Maritime Administration, for the General Bureau “Customs,” etc.;
- Unified communications network for exchange of information and network management, as integral part of the “Ekran”;
- Specialized airborne surveillance post capable of transferring data and surface picture to the land-based segments of the system.

Our assessment is that the creation of such a system will meet the requirements of all concerned authorities and will provide for effective control of shipping, protection of sea borders, search and rescue operations, prevention of ecological disasters, countering contraband and drug trafficking.

According to preliminary plans, the development and the initial operational capability of a unified coastal system for control of navigation, having the described functions and structure, will create prerequisites for:

- Significant decrease of losses for Bulgaria caused by smuggling, illegal immigration and unsanctioned use of natural resources in the territorial waters and in the exclusive economic zone of Bulgaria;
- Shortening the time needed for SAR operations by 40-60 percent, that will lead to increased probability of rescuing people and craft in distress while reducing the expenses for such operations by 30-50 percent;
- Compared with the expenses for the present organization, the installation of a single type, reliable radar systems and means of communications will allow 30-40 percent savings of finance needed for maintenance and operation;
- Bulgaria will implement its international obligations, including those for the development of the global system for rescuing at sea GMDSS.

Potential for cooperation among Black Sea countries

The assessment of the Bulgarian Navy is that there is a considerable potential in the integration of the Bulgarian automated information system “Ekran” with similar systems of other Black Sea countries. The purpose of such integration of automated systems supporting naval activities, as well as activities of border and customs authorities and maritime administrations would be primarily focused on cooperative activities in border security and SAR.

We assume that the needs of the responsible authorities in other Black Sea countries are similar to the ones described in the previous section. Achieving effectiveness in the functioning of these agencies is possible only if the needed information with adequate quality is received in time. Furthermore, effectiveness is facilitated when these agencies receive information not only about contacts in the respective national Area of responsibility but, when feasible, from the Black Sea region as a whole.

Up to now, the collection of information for maritime contacts and its utilization by the competent authorities of the Black Sea countries have been accomplished only in the framework of their national surveillance systems. Basic disadvantage of this way of operation is the lack of information in a country for the traffic of vessels, which will visit other countries’ ports or will just use the right of transit passage through its territorial waters. There is often lack of basic information, thus it is not possible to determine the port of origin and port of destination or initial and final ports of call of vessels, type of cargo, especially for vessels carrying hazardous cargo, etc. Such a lack hampers considerably control of shipping and rendering assistance to ships in distress at sea.

For example, a few years ago the Bulgarian Navy conducted unsuccessful search of a ship transporting particularly hazardous cargo, being reported to intent to dispose of it in close vicinity to Bulgarian territorial sea. Subsequently, we find out that Turkish authorities did not allow access of this vessel to the Black Sea. The timely availability of this information would have saved us

significant resources and efforts.

In addition, there have been numerous occasions when international cooperation and mutual assistance have been needed in conducting search and rescue operations.

In order to overcome these disadvantages we propose to study the possibility of regular mutual exchange of information among the Navies of the Black Sea countries and to develop jointly a suitable model for cooperation. We understand that this is not a trivial task. Even for a single country, e.g. Bulgaria, the accomplishment of this complex task requires that a number of organizational and technical problems be solved at the level of Government. Nevertheless, we believe that when there is goodwill, the difficulties may be overcome, even though that may require considerable time and efforts.

It is necessary to reach an agreement among the respective state authorities of the Black Sea countries on the transfer of certain type and volume of information. This agreement has to regulate:

- Nature and volume of information to be transferred;
- Government structure that will prepare, send, receive and use the relevant information;
- Methods and channels of information exchange.

From the organizational point of view, it will be necessary to: [5]

- Determine each country's agency that will be in charge of this project;
- Set up a collective authority to organize and control international cooperation activities and exchange of information;
- Work out the necessary regulating documents;
- Provide the needed financial and technical means.

Technically, it is necessary to solve the following issues:

- To plan and set up the necessary communications networks, connecting the naval information systems of the participating countries and providing transfer of information;
- To ensure technical compatibility among the automated information systems of the Navies of the Black Sea countries;
- To standardize forms and documents for exchange of information;
- To set up an information database.

The commencement of these activities may be gradual, starting with the most essential – creation of a sound mechanism for coordination and exchange of information among existing systems. Next, we need either to continue with the adaptation of existing systems to provide interoperability or to

approach jointly the creation of a unified automated information system of the Navies of the Black Sea countries.

Conclusion

Bulgaria, as one of the initiators for networking the naval information systems of Black Sea countries, is ready to take the initiative and to organize a meeting of a Working Group with representative for all interested countries. Initially, the Working Group would consider organizational and technical problems for the realization of the project. We believe it is possible to organize such a meeting in 2001 in Varna, Bulgaria.

I personally believe that the creation of a unified system for control and information exchange among Black Sea countries will contribute to the improvement of navigation safety in the Black Sea, will increase the operational effectiveness in the control of shipping, will improve the cooperation among our Navies and, as a result, will strengthen the confidence among the countries and the stability of the region.

Notes:

1. This article is based on a presentation of the Chief of Staff of the Bulgarian Navy Vice Admiral Peter Petrov to the Third COMBLACKSEANAVMET (Istanbul, Turkey: 18-21 April 2000).
2. For a comprehensive analysis of the relation between defense reform and force modernization, and the Bulgarian experience in particular, the reader may refer to the article in this volume of *Information & Security* by Todor Tagarev, “Prerequisites and Approaches to Force Modernization in a Transition Period.”
3. Until 1999, the respective organizations of the two ministries were considered part of the Bulgarian Armed Forces. Although they were not subordinated to the Chief of the General Staff in peacetime, planning, operations, and modernization were coordinated more efficiently.
4. The name translates literally as “Screen” or “Shield.”
5. The article by Velizar Shalamanov, “C4ISR in Modernizing Security Sector in Bulgaria and South-Eastern Europe” in this volume provides comprehensive discussion on the cooperative C4ISR development and its role in promoting regional security.

Vice Admiral **PETER PETROV** is Chief of Staff of the Bulgarian Navy since 1998. He is 1974 graduate of the “N.Y. Vaptzarov” Naval Academy in Varna, Bulgaria, and 1982 graduate of the Naval Academy (Command and Staff College equivalent) in Sanct Petersburg, Russia. In 1995 Admiral Petrov graduated with distinction the Senior Officers’ Course at “G.S. Rakovsky” Defense and Staff College in Sofia, Bulgaria. He has served in a variety of command positions in the Bulgarian Navy. In the 1997-1998 time period then Rear Admiral Petrov served as Deputy Chief of the General Staff of the Bulgarian Armed Forces.

BACK TO TOP

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

Towards Creation of a Unified Information System of the Navies of the Black Sea Countries

Peter Petrov

Keywords: ComBlackSeaNavMet, BlackSeaFor, GMDSS, cooperative security, South Eastern Europe, Black Sea security.

Abstract: The cooperation among the Navies of the Black Sea region has a significant, and as yet underutilized potential to deal with the new security challenges. In this article the Chief of Staff of the Bulgarian Navy describes the non-traditional challenges in front of the Bulgarian Navy and other governmental agencies, and the role advanced IT may play in facilitating their effectiveness. Building on that experience, Vice-Admiral Petrov proposes a regional initiative in establishing a unified Black Sea information system. He analyzes functional, organizational and technological aspects of the project, defines priorities in its development and proposes initial implementation steps.

full text

Author: **Alexi Naidenov**
Title: **Computer-aided exercises in training commanders and HQ staff: Note on Bulgarian Experience**
Year of issuance: **2001**
Issue: **Information & Security. Volume 6, 2001, pages 105-114**
Hard copy: **ISSN 1311-1493**

COMPUTER-AIDED EXERCISES IN TRAINING COMMANDERS AND HQ STAFF: NOTE ON BULGARIAN EXPERIENCE

Alexi NAIDENOV

The increasing complexity of the problems, facing the society and the military, the limited resources the armed forces operate with, as well as the overwhelming flow of information all call for increasing efficiency and effectiveness training of the staff, involved in decision making. That, among other things, will help them develop agile and inquisitive personalities.

The demanding nature of the command in a complex environment requires constant training that creates extreme situations developing even faster than real-life ones. The point is to work out a mechanism for fast and adequate reaction to problem situations by putting a man in conditional and probable situations created by imitation and modeling.[1] The immediate outcome of this is the adequate reaction to the presented extreme situation. This concerns mainly the officers and HQ staff of the Bulgarian Armed forces, because the shortening education and training period concurs with the widening range of requirements put forth.[2]

Both the transition to a new organizational and staff structure and the increasing importance of the officers' professionalism call for quantitative and qualitative improvement of the training of HQ staff, as well as the HQ command exercises. Furthermore, this has to be accomplished in times of continuous shortage of funds. Improving the HQ's organization, lowering spending as much as possible and eliminating the risk of human loss or environmental damage is a vital issue for any military organization. These requirements limit even more both the chances of proper utilization and putting into practice of the skills gained to date and the testing of the training process and combat readiness. The main way for dealing with these circumstances is the search for, and application of, new training programs for the commanders and headquarters' staff (HQS) that will create working conditions adequate for the command of the military forces in near combat conditions.

The experience of the armed forces of NATO member countries and the limited Bulgarian experience show that main way of improving the commanders and HQS preparation is the implementation of computer-aided exercises.

The computer-aided commanders and staff exercises are a modern and effective training method for the operational and tactical formations.[3] They aim at developing certain skills in the commanders and HQS that will later help them optimize the current HQ procedures and functions. In the armed forces of NATO member countries the computer-aided exercises comprise approximately sixty percent of all exercises and this figure rises each year.

Depending on the training objectives, the problems solved, the trained staff, the precision of presenting the forces, weapon systems and location, and the impact of other factors, the computer-aided exercises can be categorized in three thematic groups: [4]

1. Group exercises;
2. Comprehensive exercises;

3. Detailed exercises.

The group exercises have a limited number of participants and hierarchical levels. Using a comprehensive simulation model, they deal with a small number of issues that represent just a part of the combat. The modeling is quick and allows us to concentrate on the aims and objectives of the exercise.

The comprehensive exercises have broader objectives and all staff members with functional duties, pertinent to achieving the objectives, take part in the exercise. In these exercises the separate combat episodes are not emulated in detail but are analyzed instead from a broader perspective. The operation of training HQS is in real time

The detailed exercises have specific objectives and involve a great number of organizational units. In the process of their modeling lower organizational levels and larger number of factors, that impact the combat, are being acknowledged. They use a system of models of types of military forces, Special Forces and weapon systems characteristics. The exercise is conducted in real time.

With the help of this table the commander (supervisor) can choose what type of computer-aided exercise to carry out, with the headquarters under his command, while taking into account the preparedness level, number of participants, objectives and available materiel.

Table 1 summarizes the characteristics of the different groups of computer-aided exercises (CAX):

Type of CAE	*Number of participants*	*Level of difficulty*	*Price*	*Time*	*Needed preparation*	*Difficulty of the objectives*	*Number of tasks*	*Adequacy of the model*	*Duration*
Group	small	low	low	accelerated	short and simple	limited objectives	small	relatively comprehendsive	short
Comprehensive	average	average	average	real/ accelerated	moderate	broad objectives	average	relatively comprehendsive	average
Detailed	large	high	high	real	long and complicated	diverse and complicated	large	detailed	long

Functionally, the technology used in computer-aided exercises should meet the following requirements:

- To come as close as possible to the HQ’s real life operational environment;
- Commanders and HQS should not be required additional skills in order to perform their duties, i.e. they should use the standard HQ’s operational and collaborative procedures;
- Each command staff trainee should comprehensively perform his or her functional duties while organizing the combat operation;
- It should allow the use of graphical information systems and other modules for target analysis, in the area, while facilitating the objective, situation assessment and following HQ actions, i.e., the system should be open and expandable.
- To display real time graphical environment as close to reality as possible;
- Real time display and processing of information should be according to plans;
- The results of the trained commands and orders should be displayed in real time;
- A capability for easy interaction should be provided so that the planned HQ objectives are achieved;
- A capability for statistical output and data storage of different decisions should be provided in order to compare, analyze and study the results of a specific decision made.

The current simulation system used for computer-aided exercises in the Bulgarian armed forces is tested and adopted in 1996. It is designed to perform HQ command computer-aided exercises at the level of all arms brigade. The system provides good educational capabilities. However, the systems' mathematical model has the following drawbacks:

- Lack of an integrated database;
- Lack of common mathematical logic;
- Lack of common algorithmic structure.

As a result we can only achieve part of the commands' general objectives.

This is also a reason for us to make a determined effort to develop simulation systems in a relatively short period of time (until 2003) so that the following objectives are achieved:

- Improving the quality of the training of HQS and forces in accordance with the Concept of National Security, the Military Doctrine of the Republic of Bulgaria and the Plan for Organizational Development of the Bulgarian Army until 2004;
- Providing for the operational compatibility with the armed forces of NATO member countries;
- Bringing the training in compliance with the current legislature and criteria founded in the qualification records and requirements for training HQS;
- Reaching optimal utilization of HQS and maximal command efficiency by means of multilateral modeling of major combat processes;
- Unifying (synchronizing) the separate elements of the military education such as: syllabus, methodology, study facilities, qualification, etc., in order to achieve the major objectives of training commanders, HQS, armies and forces;
- Developing a unified and effective model for training commanders, HQS and troops while keeping in mind the qualitative changes in the military science and development of information and management technologies;
- Taking part in certain joint exercises with NATO and "Partnership for Peace" (PfP) member countries and the necessary for that preparation and regular participation in national training exercises similar to those carried out with the neighboring PfP member countries.

The realization of the latter corresponds to decisions of the Washington Summit of NATO in April 1999. The Nrth Atlantic Council issued a resolution for further development and utilization of new defense information technologies and secure integrated computer communication network among PfP member countries. It is envisioned that the network will be based on three major subsystems:

- Consortium among the military education facilities and so unifying their curricula;
- A unified network of functional crisis management centers;
- A network of the general headquarters used for performing HQ command computer simulated exercises.

Last year, in compliance with that resolution, together with PfP member countries, a shared HQ command exercise was carried out called "Peace Shield 2000". The exercise was particularly important for the Bulgarian armed forces because one of the centers was situated in the country. The exercise was carried out between the 8th and 22nd of July 2000. There were 21 participating countries divided in two multinational brigade headquarters, acting as multinational battalion headquarters, and several formations all operating on the battlefield.

The aim of the exercise was both to organize the multinational headquarters and, in reality, to resolve issues on tactics improvement and methods for conducting peacekeeping operations by means of computer modeling, implementation of new information technologies and communication systems.

The exercise was conducted on the “Javoriv” training facility near Lvov, Ukraine, using four remote command posts, one of which was the Command and Coordination Center. The other three command posts were Combat Preparation Centers in Bulgaria, Estonia and Ramstein Air Base – Germany. There were two battalion headquarters – Bulgarian and Moldavian.

In the course of the exercise all trainees faced the following major objectives:

- Organizing the multinational brigade headquarters taking part in the peacekeeping operation while developing general procedures on conduct (rules of engagement) and planning;
- Improving the command and control methods for peacekeeping operations;
- Improving the readiness to organize and provide for operations while gaining experience in similar operations and exercises;
- Improving the collaboration among participants in peacekeeping operations;
- Allowing staff members to exchange information on peacekeeping operations;
- Encouraging mutual trust and respect among staff members of the participating countries;
- Implementing and improving the technology that supports the exercises on the “Partnership for Peace” Program.

Organizers of the “Peace Shield 2000” exercise were the European command of U.S. Forces, the National Guard of Illinois and the Ukrainian MOD.

The exercise was carried out in five major stages as follows:

I. Deployment of the Combined Peacekeeping Forces (CPKFOR-00) to the ordered location.

II. Preparing CPKFOR-00 for organizing the multinational command structure and establishing standard operational procedures on all HQ levels. Training units to perform the major objective for a given location.

III. Replacement of CPKFOR-99 command with that of CPKFOR-00. Establishing the temporary joint-activities headquarters until taking tactical control over the units and conducting orientation meetings of all commanders on the operation and their responsibilities.

IV. Conducting the peacekeeping operation.

V. Devolving CPKFOR-00 powers to the Federal Government after holding elections, reaching long-lasting peace and conducting redeployment to national bases.

A satellite connection was established, between the Center for Combat Training of the U.S. Army in Ramstein Air Base and the “Yavoriv” training facility near Lvov, Ukraine, for the command of both the multinational brigade and battalion headquarters. Hosting countries also provided ISDN channels among all remote command posts in Bulgaria and Estonia allowing diverse means of communications. High-speed broadband networks integrating different means of communications, such as telephone, fax, video data transfer and new multimedia services, combining text, sound and picture in various applications, remodel completely the way of managing, processing, transferring and exchanging information and so gave an advantage in terms of time and distance.

During the exercise the Bulgarian and Moldavian battalion headquarters used the following ISDN services:

- Basic Rate Access (BRA) also known as 2B+D provides a standard subscriber line allowing simultaneous communication on both channels with transfer speeds of up to 64 Kbit/s for the ‘2B’ channel and 16 Kbit/s for the ‘D’ channel;
- ISDN telephone – modern multifunctional telephones equipped with message and control display;

- Telecommunications services – Information exchange between two or more subscribers (trilateral and conference connection);
- Multiple Subscription Number (MSN) – ISDN, characterized by flexible number determination.

While organizing the exercise the following advantages of the ISDN lines became apparent:

- High quality and dependability of the connections. The transfer of digital data was hardly affected by noise and errors on the line. Wherever errors occurred, in the network, the transfer was relocated to alternative routes and, thus, did not affect the exercise;
- Transfer speed. Both communication channels, each carrying 64 Kbt/s of data, provided speech, text, graphic, and video data transfer using a PC;
- One line gives access to all services, similar tariffs and uses a single long-distance connection interface;
- Fast dialing. The digital equipment allowed much faster dialing the brigade headquarters – a matter of 3 to 4 seconds;
- Single standard. EURO standard valid in our national network assured the compatibility of the ISDN networks of all countries, end devices and equipment.

The exercise uses the JCATS 2.0 (Joint Conflict and Tactical Simulation) system that is multilateral, interactive, high-resolution and comprehensive. The ways of using this new model can be summarized as follows:

- Modeling operations, usually military operations other than war, that combines economic, social, military, and political activities by using comprehensive, strictly specific and characteristic of the operations' local area database;
- Simulation of different types of combat;
- Modeling combat and non-combat activities in cities by using detailed records of existing buildings, location characteristics, roads and communication facilities.

The JCATS 2.0 model covers the levels from company to brigade inclusively and allows the battalion headquarters to execute four to seven tasks daily, including:

- Refugee convoy;
- Humanitarian aid convoy;
- Controlling mass demonstrations;
- Giving first aid to wounded and injured personnel;
- Designation of mines and mine fields; mine clearing;
- Detaining weaponry and drugs traffickers;
- Detaining terrorists;
- Water, fuel, food and ammunition supply;
- Evacuating wounded and injured personnel;
- Supplying mass, religious and holiday activities with food.

All those tasks were developed with the simulation system. They all required the input of specific objectives, unit collaboration procedures, and subalterns' duties.

Besides using the models' role-playing feature, battalion HQs solved the following problems:

- Conducting negotiations with mayors and other official representatives of the local government;
- Giving first aid to young mothers and sick children;
- Organizing the cooperation with the local police, paramilitary organizations and formations.

For the first time the exercise featured WEU and NATO candidate member countries. The participation of the Republic of Bulgaria, as a hosting country of one of the centers of the exercise, was highly appreciated by both the organizers of the exercise and the European command of US Air Forces. The exercise allowed the participating Bulgarian officers to gain skills and experience while working in multinational headquarters and to learn the operational procedures for conducting peacekeeping operations.

The conduct of the computer-aided exercise and field exercise proved to be highly effective in training headquarters and units for achieving mission objectives.

The computer-aided exercise pointed out a number of advantages of the simulation system for training commanders and HQS. They can be summarized as follows:

- Bringing the working environment as close as possible to a real combat situation. The trainees took full advantage of this fact and used all systems' capabilities available;
- In that kind of exercises organizing the HQ and its capability to quickly assess the current situation is of greatest importance. The systems capability of multiple repetition of certain situations proved clearly that HQ Command efficiency is of paramount importance;
- The Command of the exercise skillfully guided the actions of the imitation groups so that the trained HQ could act in a dynamic environment demanding untraditional solutions;
- The decision making process, unit command and bilateralism of the exercise were brought as close to reality as possible;
- The simulation system allowed the Command of the exercise to experiment with some of the HQ's tasks that were considered problematic. The use of this tool also generated a more efficient training strategy.
- The Command Center was able to provide analysis and documentation for the complete course of the exercise and also records for the trained situations and orders. All that was used for the daily and final breakdown of the exercise. In addition, the archiving of the results of the exercise gave the commanders detailed records for later usage.
- The objectivity of the modeling system stimulated the resourcefulness of each commander and the models' output, for each decision in the peacekeeping operation, made them more confident. In addition the analysis of different situations and variants encouraged their creative thinking and learning.

In conclusion we can say that the analysis of the conducted exercises and our experience in the Partnership for Peace Program undoubtedly proved that computer-aided exercises are a new and promising way of training officers and HQS. At the same time, they must not be accepted unconditionally and as utmost value - real life human experience, gained in field activities, should not be brushed aside. In the future we must achieve a proper balance between field and computer aided exercises so to provide for the most effective training and commanders and staff of headquarters.

Notes:

1. G. Brewer and M. Sbubik, *The War Game: A Critique of Military Problem Solving* (Cambridge, MA: Harvard University Pres, 1979).

2. Described in detail in Nikolay Vraikov and Alexi Naidenov, “The Computer- Aided Exercise – An Alternative of the Conventional Exercises in the Armed Forces,” *Information & Security: An International Journal* 3 (2000): 119-131.
3. Valentin Penev, "Simulation Modeling in Military Affairs: Status and Perspectives,” *Information & Security: An International Journal* 1, 1 (Summer 1998): 91-102.
4. Alexi Naidenov adn Nikolay Vraikov, *Computer assisted Exercises* (Sofia; Military Publishing House, 2000).

ALEXI NAIDENOV is Colonel in the Bulgarian Army, chief of “Exercises, Training and War games” Department at the Operations Directorate of the General Staff. In 1977 he graduated from “V. Levski” Army Academy in Veliko Tyrnovo, Bulgaria. Then he served in a number of Land Forces units. In 1986 he graduated from “Frundze” War College in Russia. After that he consecutively took positions at various staffs – Corps HQ, Land Forces Headquarters and General Staff of the Bulgarian Armed Forces. Since 1993 he is involved in designing and implementing the policy of using simulation systems in staff and troops training. E-mail: aleksi_NAC@yahoo.com

BACK TO TOP

Computer-aided exercises in training commanders and HQ staff: Note on Bulgarian Experience

Alexi Naidenov

Keywords: CAX, PfP exercise, Peace Shield 2000, military training, simulation-based training, multi-national peace support operations.

Abstract: Computer-aided exercises (CAX) are a valuable tool for training under resource and environmental constraints. CAX allow to train realistically commanding officers and headquarters for participation of a broad range of missions. This article describes the recent experience in using distributed CAX to conduct a Partnership for Peace exercise of a multi-national peace support operation. Touching briefly on the technical setting for the exercise, the author puts the emphasis on operational and training advantages and limitations of CAX systems. The experience is assessed in the framework of traditional Bulgarian understanding of the role of CAX.

full text

Author: **Greta Keremidchieva and Plamen Yankov**
Title: **Challenges and Advantages of Distance Learning Systems**
Year of issuance: **2001**
Issue: **Information & Security. Volume 6, 2001, pages 115-121**
Hard copy: **ISSN 1311-1493**

CHALLENGES AND ADVANTAGES OF DISTANCE LEARNING SYSTEMS

Greta KEREMIDCHIEVA and Plamen YANKOV

Distance learning has been around for ages. From the moment you decide you would like to continue your education, the Internet can provide access to detailed information about the many institutions and distance-learning courses currently available to you worldwide – information about the teachers, deadlines, grants and fees. A course web site might include a syllabus, a summary of lessons, notes, links to helpful sites and related research, projects done by students, model assignments and a long list of etceteras considered impractical under the more traditional system. The interactivity of the Web allows for spontaneous feedback and rapid change, without the hassle of endless photocopying.

During the course of studies, many different applications of the Internet may be used. For example, distance-learning courses now customarily take advantage of the speed of basic e-mail to forward reading lists, assignments and course support materials. Communication with the course instructor is more efficient this way and questions can be handled more swiftly. According to evaluations from the fall of 1996 at the University of Illinois, the students reported increased their communication with professors 64 percent and the quality of interaction with instructors 57 percent. At the same time the faculty reported increased communication with students 92 percent and the quality of interaction with students 88 percent.

Contact between classmates becomes feasible, making group tasks and project work real options for the isolated distance learner. It should also be much easier to stay in contact and keep abreast of developments after the course ends. Post-course support and follow-up can take place via discussion boards or mailing lists at your convenience. The survey mentioned above proved that communication between students increased 43 percent, whereas students commented "I learned much more than I ever had due to the high interaction between student-student and student-teacher."

As Eastmond defines the philosophy of distant learning, it "breaks down barriers for adult learners and shifts emphasis from how or where learning takes place to learner outcomes". A further comparison between traditional and distributed learning will mark differences in various aspects. While in the traditional process teachers lecture and students listen, in the process of distributed learning teachers guide and students are active. Individual work has been replaced by teamwork. Fact-centered learning of specialized subjects has changed into problem-centered integrated studying. Furthermore, in the old classroom teachers were the primary resource of materials and knowledge, while the new method

makes multiple resources available to the student. Regarding the teaching materials, what used to be predominantly print media became a mixture of media.

All teachers, from the most traditional to the most innovative, can find uses for the distance learning method in their teaching. There is plenty of opportunity for short, quick practice activities as well as full-blown tasks and extensive projects. Though the distance learning method of teaching will not substitute for a good teacher completely, it will immensely enrich the classroom resources and can be used whatever the teacher's approach to language teaching.

Two factors are essential to computer-mediated learning success, both for faculty and students. First, this is prior computer and networking background, and second, the existence of a support person or team. Despite the ease of point-and-click technology, teachers should plan to spend sufficient time using the technology for themselves – both as a resource for materials and a teacher development tool – before trying to use it with students. Most of the students are experienced users of the Internet. On the other hand, certain students face computers with intense anxiety, sometimes to the point of technophobia. This does not make using the technology unworkable, but requires very skillful handling.

Connected to the problems in realization of projects for distance education it is important for their software designers to apply some of the proven in action current approaches for constructing network software management system of distributed system and application software, designed to support the process of distance education and existing strategies for controlling dynamical data exchange in the world wide computer networks.

Agent/ Manager Paradigm – Most of modern network software management solutions are based on the agent/manager paradigm, in which management communication occurs between a manager and an agent system, as illustrated in Figure 1.

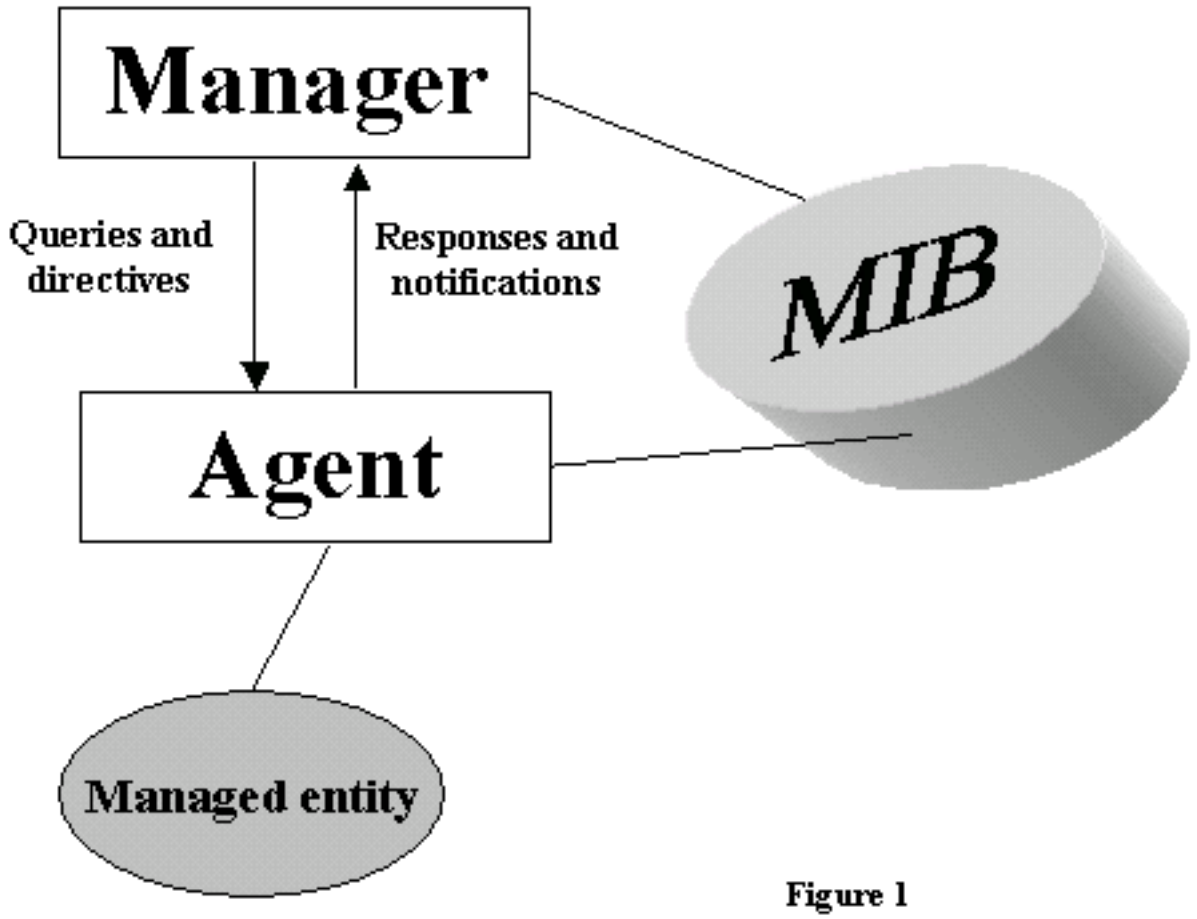


Figure 1

Practically in many cases specific management system may function as a manager for some applications and as an agent for other applications. The agent/manager paradigm is similar to the client/server paradigm except for some minor differences.

Usually, the manager is analogous to the client and the agent to the server. But in some cases, event reporting can be prearranged at the configuration level so that the agent reports events without explicit request from the manager. This represents a departure from the classical client-server model, because the roles played by the agent and the manager and the agent are switched. The agent initiates a reporting action, so it acts as a client. The manager reacts to the agent's action, so it behaves like a server. Swapping the roles is not part of a client-server model.

A manager is a software program that can query agents, receive responses from agents, and send directives to them. An agent is a software program (often residing on the managed entity) that responds to manager requests and performs management functions on the managed entities (communication and application software resources capable of being monitored and controlled). A management information base (MIB) is a conceptual representation of information related to a managed entity and how users can access it.

The agent acts as an interpreter of information resources contained in the MIB, providing filtering of the information and informing the manager about autonomous events that occurred. Communication between agent and manager is performed as a set of requests, responds, and autonomous messages as defined by specific standards. According to OSI, MIB is a collection of managed object classes defined in the special purpose notations described in the guidelines for the definition of managed

objects (GDMO), ITU-T Recommendation X.722. TMN standards are much more complex and more difficult to implement than SNMP. However, they are much more powerful and efficient for large-scale networks. There is an objective need of a proliferation of proprietary interfaces at network elements. It and some other reasons have led to the adoption of Common Object Request Broker Architecture (CORBA) in network software management, because standard distributed object technologies including CORBA offer low-cost development platforms and tools. Moreover CORBA is vendor independent and is thus the logical choice for systems that must operate in a heterogeneous environment. With CORBA agents in all network elements (NEs), we can develop a purely CORBA-based network management system. However, the CORBA-based architecture reuses existing MIB specifications using gateways between CORBA-based network management applications and CMIP/SNMP-based network elements. The term agent is highly overused. On the one hand, we have systems like SNMP and CMIP agent that are nothing more than servers providing data to their clients – management applications. On the other side of the spectrum, there are expert systems with huge knowledge bases, which are also considered agents due to their intelligent behavior. Talking about an intelligent agent we have in mind a computational entity that acts on behalf of others, is autonomous, is both proactive and reactive, and exhibits a certain degree of ability to learn, cooperate, and move. A “client” delegates to an agent certain tasks that are to be achieved without, or with a minimum of, his further involvement. After receiving the task, the agent acts autonomously following certain algorithms. Using their skills, agents proactively try to attain the goal defined by the assigned task. They can acquire their skills by being told (education) or through expertise (observation). Agents react to changes in the available data by modifying their plans. They acquire and modify their knowledge in response to experience and exchange of information. They also communicate to share their knowledge and collaborate in attaining their goals. Agents may have to be mobile to achieve their goals. A mobile agent is an agent that can be moved between execution environments. The use of mobile agents addresses efficiency, reduction of network traffic, asynchronous autonomous operation, local interaction with real-time systems, support for heterogeneous environments, on-line extensibility of services and convenient development paradigms. It is a common opinion that creating distributed systems based on mobile agents is relatively easy.

The conclusion is, that we have to be ready to see in the near future a fast growing number of applications of the above described and similar technologies for solving the current problems of distance education learning software.

Distance learning as a form of training has been recognized and is gaining speed in the military sphere. The Training and Education Enhancement Program (TEEP) outlines that distance learning of English, through the present and future electronic networks, could be an option, as mentioned earlier, for Partners to access basic or specific English Training modules. This area will be further explored as a part of TEEP Distributed Learning and Simulation.

The authors of this article have participated in the designing of software for a project for the system named Partnership for Peace Learning Management System (PfPLMS). This is a software development project that aims to provide a free or low cost solutions to Partnership for Peace Nations organizations, to evaluate the benefits of using Advanced Distributed Learning (ADL) technology to assist them in the quality, throughput, and effectiveness of their training programs. It attempts to focus in on the requirements and particulars of organizations working under the auspices of the PfP Consortium of Defense Academies and Security Studies Institutes, as the particular challenges seen in

training military officers and civilian leadership is of special importance politically to the stability of PfP Nations.

The system itself can be described as a software repository that can hold, manage and facilitate the interaction of student-instructor relationships around a particular course. It combines catalogue features, coarse design features, including re-use of existing material, and automated procedures for students to interact with course material, and course instructors located elsewhere.

The project differs fundamentally from other development projects, in that a definitive statement of work, or compilation of users requirements did not exist prior to the initial stated requirements for this system. The background may be divided into two sections: emerging technical requirements to satisfy the MOU concerning Advanced Distributed Learning, and a prototype project begun to offer a single course. As part of the process of 'deconstructing', or interpreting the MOU, the primary agencies responsible for oversight of the MOU perceived the MOU to call for the design, creation, population, and long term maintenance of a centralized repository of Distance Learning Courses, to be:

1. Used by Partner organizations in their attempts to further their interoperability and integration into NATO/Western European engagement.
2. As much as possible to adhere to emerging US DoD standards for Distance Learning (SCORM), to further future interoperability amongst allies.
3. To lay the groundwork for an eventual "virtual defense academy", where courses affecting military and civilian leaders could be maintained virtually, encompassing courses, instructors, and students from various locations, positions, etc.

As part of this effort, the Joint Planning Committee comprised to oversee the implementation of this MOU primarily concerned themselves with identifying the applicable standards, courses that could be made available, and teams to assist course providers in the conversion of these courses into an online system.

From a technological point of view this project (Version 1) can be described as a distributed in INTERNET combination of system and application software. As a database management software is used Postgress, contacted from scripts using SQL style statements, which in our opinion is appropriate for relatively small software systems. Almost all of the scripts for communication with databases and Internet browsers are written using Perl language and CGI (Common Gateway Interface) standard. In order to speed up the work of the application software, in our opinion, it would be better if Perl’s DBI modules were used. The result would be, first, higher speed transactions between the databases and user’s site in Internet, and second, it would provide more standard access to the databases. The last remark is important, since this is intended to be an open source project and in the future different designers from different software teams and different countries should be able to add in a more uniform way their contribution in the development of this project.

Efforts have been made to modify the proposed schema for this current cycle to be more in line with mandatory object descriptors as advocated by SCORM. Similar changes to improve the ability to exchange information could also be accommodated. It should not, however, be confused that the

particular requirements for an LMS for a PfP audience may differ in its implementation than that designed for a US or Western European audience. Efforts should be made to ensure compatibility where possible, but functionality, user friendliness, or real world constraints such as communications, local equipment, language barriers, etc., should not be sacrificed to ensure full compliance.

Notes:

1. *PfP Learning Management System. ESSO Project,* Working Paper, (Consortium of Defense Academies and Security Studies Institutes, IT Working Group, September 2000).
2. David J. Sidor, "TMN Standards: Satisfying Today's Needs While Preparing for Tomorrow," IEEE Communications Magazine (March 1998): 54-64.
3. J. Patrick Thompson, "Web-Based Enterprize Management Architecture," IEEE Communications Magazine (March 1998): 80-86.
4. Neal Calanni, "A New Breed of VPNs," Business Communications Review International (October 2001): 50-53.
5. James F. Kurose and Keith W. Ross, *Computer Networking: A Top-Down Approach Featuring the Internet* (Addison Wesley, 2001).

GRETA KEREMIDCHIEVA: MA (1985 English philology) degree from Sofia University. Specialization in Management of English Language Training, USA, Military Materials Design, UK, English Language Testing for Military Personnel. Currently, she works as Chief of English Language Training Department at the “Rakovski” Defense and Staff College.

PLAMEN YANKOV: MSc (1985 Radio Electronic Equipment of Airplanes) Air Force Academy; MSc (1991 Computer Science) Technical University Varna. Specialization in Computer Networks Management, Keesler AFB, USA; Arms Control Procedures and Information Systems, Germany. Currently, he works as a researcher in the Defence Advanced Research Institute, “Rakovski” Defense and Staff College.

BACK TO TOP

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

Challenges and Advantages of Distance Learning Systems

Greta Keremidchieva and Plamen Yankov

Keywords: distributed learning, network management system, learning management system (LMS), manager/agent paradigm, intelligent software agent, client/server.

Abstract: The authors analyze the role of distance learning in the training process. Particular emphasis is placed on some problems and challenges connected to new methodology and technologies. Most ideas expressed in the article are the result of the authors' practical experience in constructing and implementing distance learning systems. Connected to the problems in the realization of projects for distance education, the article brings up the issue how important it is for their software designers to apply some of the proven in action current approaches for constructing network management software for distributed systems and application software, designed to support the process of distance education and existing strategies for controlling dynamical data exchange in the world wide computer networks.

full text

Author: **Yuliana Karakaneva and Georgy Pavlov**
Title: **Advanced Technologies for Defense Information System Support**
Year of issuance: **2001**
Issue: **Information & Security. Volume 6, 2001, pages 122-131**
Hard copy: **ISSN 1311-1493**

ADVANCED TECHNOLOGIES FOR DEFENSE INFORMATION SYSTEM SUPPORT

Juliana KARAKANEVA and Georgy PAVLOV

Table Of Contents:

Planning and operational command and control (C2) of the Armed Forces is a complex human activity. It requires gathering, integrating, analyzing and assessing a large amount of information. It also involves situation identification and assessment, making decisions in various conditions and managing their performance. The contemporary implementation of decision making information methods and tools is considered a priority way of managing information warfare - a pursuit of effective accumulation, control and use of information and knowledge.

Some of the main aspects of C2 and its information support are[1] :

- C2 processes and their information technology. support
- Developing and implementing management information environment support.
- Efficiency and effectiveness of the information environment.

Each stage of the management process uses various, electronically represented, information resources. The effective functioning of information environment becomes a main factor for management success.

The information quality criteria are clearly and precisely defined in the US Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations:

- ***Accuracy***

  Information that conveys the true situation.

- ***Relevance***

Information that applies to the mission, task, or situation at hand.

- ***Timeliness***

  Information that is available in time to make decisions.

- ***Usability***

  Information that is in common, easily understood format and displays.

- ***Completeness***

  All necessary information required by the decision-maker.

- ***Brevity***

  Information that has only the level of detail required.

- ***Security***

  Information that has been afforded adequate protection where required.

Strategy, organization, technology

The current state of affairs poses some conceptual, organizational and technological problems for the military information systems. This paper considers the information support of management problems in two main directions: conceptual (concerning Information Strategy), and technological (concerning Information Environment).

Modern command and control information systems (CCIS) are characterized by managing and processing huge amounts of information and knowledge elements of different data types in distributed communication networks. The problems in military CCIS, however, are not caused mainly by the military structures and operations complexity, but rather by the influence of three other factors: the rapidly changing conditions regarding applied technology, the operational requirements and the various user profiles.

In most cases it is not possible to design military information systems (IS), which have an overall consistent hardware and software, for conceptual and technical implementation. Contemporary operational requirements involve continuous updates and adaptations. As a result a heterogeneous environment evolves in which C2 processes have to be embedded. This complicates the system's support and induces information flow interruptions.

The new requirements for multi-national command structures in actual out-of-area missions - coalition warfare, peacekeeping and peace-making missions [2] - cause another problem. International missions have to be planned, prepared and executed within a short time frame and in accordance with actual needs. All this requires high flexibility and adaptability of CCIS.[3]

Another problem is the need for a different user-friendly profile support. An information environment has to provide direct task-oriented and problem-oriented access to the information, which is actually needed in the current operational situation. The human-machine interface is developed in modern multimedia environment.

In order to overcome the restrictions and insufficiencies of military CCIS it is necessary to make more efficient design processes based on new information technologies.

Information technology (IT)

Information technology (IT) is applied in ways that not only contribute to more effective operations, but also reflect on the operating process so that new possibilities and perspectives arise. [4]

The initial application of IT was in automating the work process - substituting humans for technology that performs repetitive tasks in a more reliable way. Indeed, the various applications of the information intensive workplace extend the individual's capability to process knowledge and apply technology while gaining experience in various new ways.

The nature of work, itself, shifts from functional to cross-functional, from individual to group, from fixed procedures to alternative paths, from structural to virtual organizations, from work groups to networks of problem solvers. The transition to an information environment inevitably leads to the transformation of the activity-level work processes.

Information technology is the primary stimulant for this transformation. It is the tool of the knowledge worker. The effective integration of information technology with work processes can lead to flattened organizations, more flexible and adaptive work processes and more reliable and responsive outputs.

This is the stimulant for most reengineering projects. They are driven by a desire to capitalize on the promise of efficiency and effectiveness that are available through the better use of information technology. The information technology integration is so important because the automation of work processes provides a qualitatively better outcome. The very definition of knowledge is changed in the information intensive work environment.

Scientific knowledge

The scientific knowledge is proving to be the most valuable type nowadays. It is a structure of statistically proven and codified laws, theorems, and procedures that either have been or could be validated and verified by an independent investigator.

Through scientific methods a set of conditions and events is observed. It is represented in an analytical form, collected for consideration and processed with the use of an analytical method. The produced data is then manipulated, presented and interpreted so that the output can be defined as information. Information, once tested, validated, and codified becomes knowledge.

Scientific methods

Advanced Information Technologies are based on a variety of tools, methods, techniques, devices and architectures. The research-workers proposed taxonomy of scientific methods, which can be used to identify and validate requirements, build prototypes, and test and evaluate software and whole information systems. [5]

In particular the information science methods are presented on Figure 1.[6]

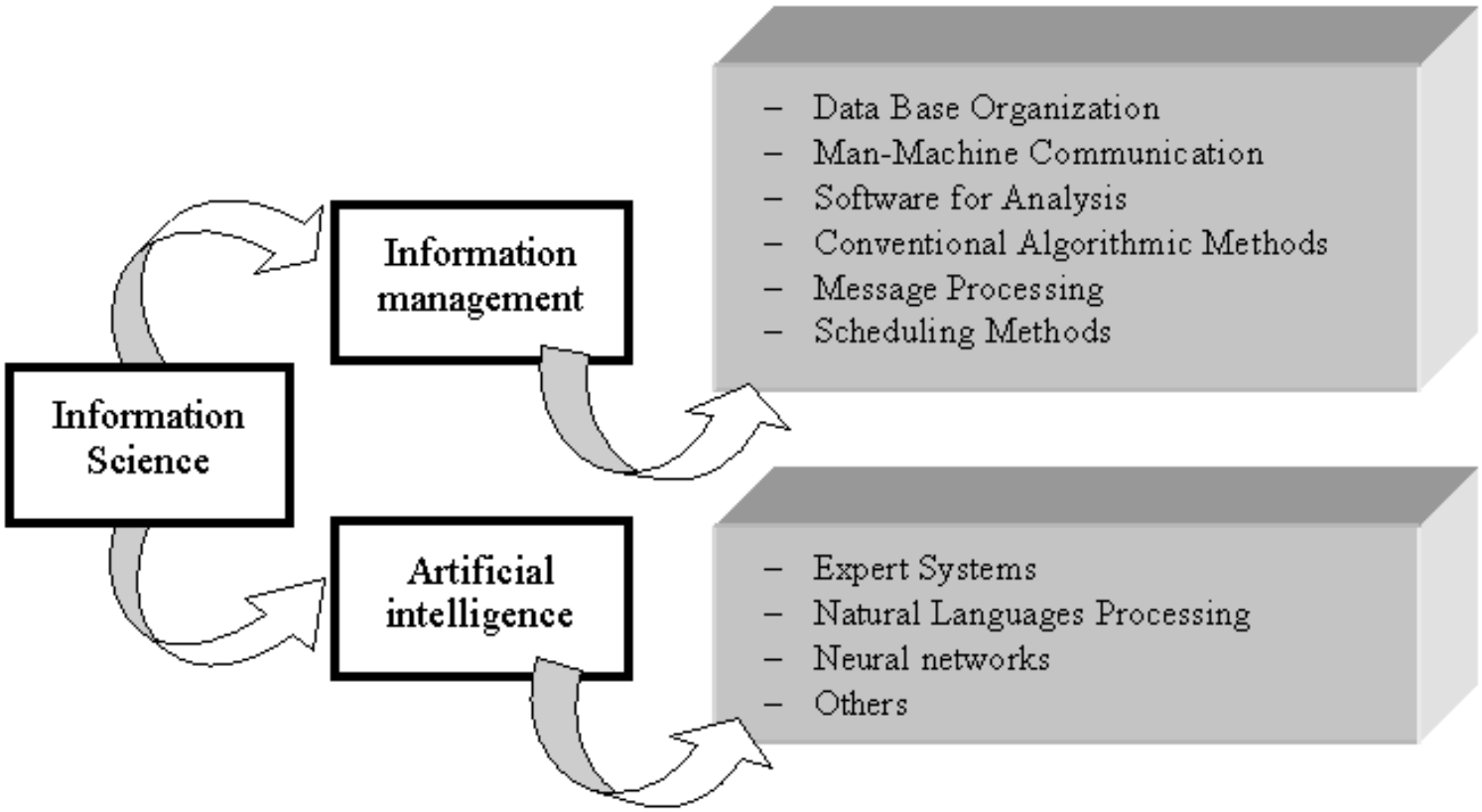


Figure 1: Relation among information science methods

For the last few years the approaches to decision support system development are knowledge based. The artificial intelligence can provide support to well-bounded problems, but it is less effective in situations with unpredictable characteristics. The latest methodology to attract attention is neural network-based models of inference making and problem solving. The neural networks are applicable to problems with characteristics that are quite different from those best suited to the artificial intelligence. They are non-deterministic, non-algorithmic, adaptive, naturally parallel, and naturally fault-tolerant powerful tool for decision making systems design.

Mission of information systems

The classic information system aims at getting the right information to the right person at the right time.[7] In today's mission environment objectives such as these are limited and short-sighted. Even the ”right information” objective fails to note whether anything useful results from the delivery of the information. We suggest the following mission as appropriate for information systems: To improve the performance of people in organizations through the use of information technology.

The ultimate objective is performance improvement - an outcome or result goal instead of a go-trough-the-steps process goal. Certainly the overall organizational performance is improved, but the means of doing it are the people or groups of people that comprise the organization. The source of this improvement is the development and use of information technology, such as computers, computer software, machine readable information, and communication technologies - computer message systems, computer conferencing, or video conferencing.

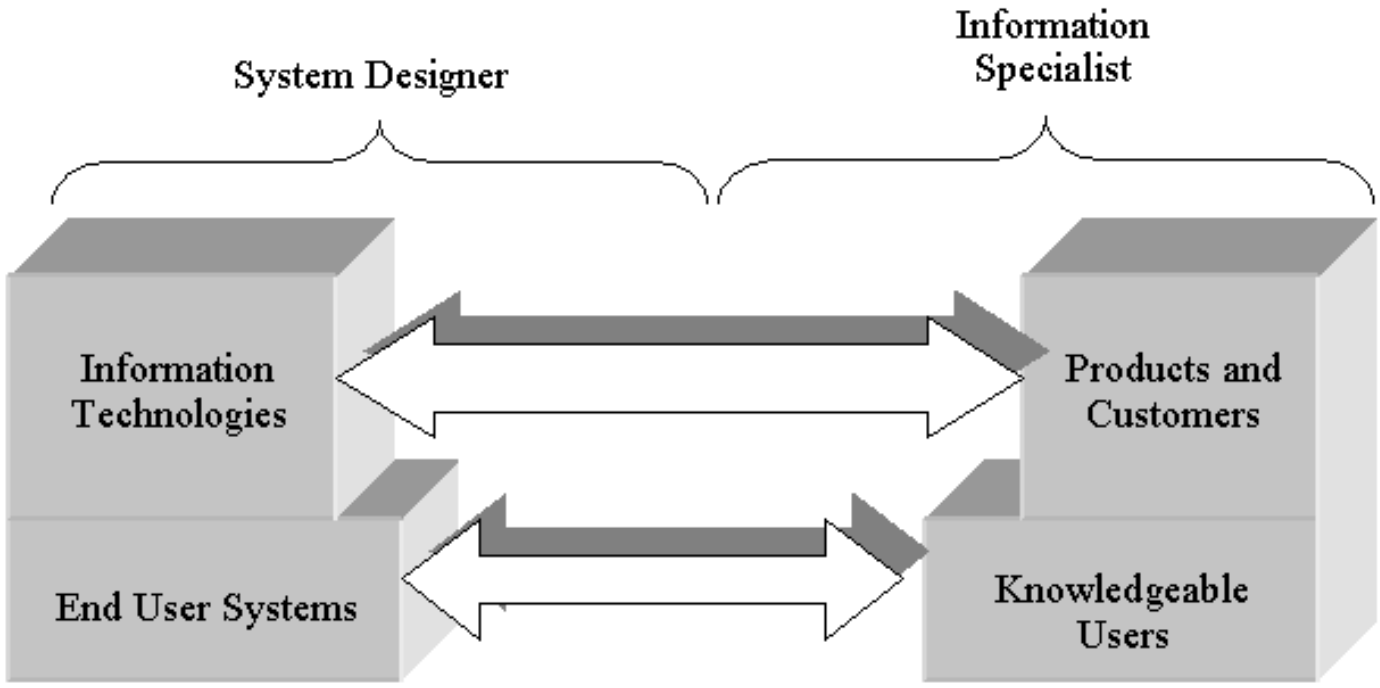


Figure 2: Relations among information experts and users

In the early days of information systems, the management support process was conducted almost entirely by a system analyst. During the past 25 years technology has become increasingly complex and powerful. At the same time the uses to which it is being applied have become increasingly sophisticated. Information systems are now viewed as system products in which users have become educated customers of the professional systems department (figure 2). The widened gap between the two boxes represents the increasingly complex process of developing and delivering the systems products. More specialization and skills are required of the system professionals to cover this wider gap. At the same time, many users are becoming so knowledgeable and computer-literate that they can deal with the computer directly and even develop their own systems. At the present time a certain segment of the technology is truly user-friendly, if any end-user languages to serve a wide variety of applications. Specific applications such as database inquiry report generation, and spreadsheet manipulation are regularly developed and used by managers and professionals, but it will be some time before end user will bear the majority of the system development load.

The main point of this discussion is that the technology is getting more complex, the applications are getting more sophisticated, and users are beginning to do some system development. The net result is that the management of the entire process is getting more complex and difficult while at the same time it is getting more important to do it well.

We use a model based on three principal elements:

- A set of technologies that represent products, developed by system department and other organizations.
- A set of users of the technology who can be viewed as users of these products.
- A mechanism for developing, delivering and installing these systems.

Strategic Information Systems

In this emerging age of the knowledge worker, there is a shift in the way, how managers perceive the utility of information systems. A hint of this transition can be recognized in information system labeling: some of the more systemic planning applications of management information systems are now labeled strategic information systems. These strategic information systems (SIS) refer to applications of information technology that are used to support or shape the policies and competitive strategy. Any such SIS that seeks to deliver sustained competitive advantages must be managed as a continuous innovation process - one that keeps recreating new advantages that drive the user's perception of exciting quality in new product features. There are two linkages for the innovative management of a SIS

and the process of system engineering. One touch point is at the start of the technology assessment where innovation is needed to discover those unique organizational attributes that can be leveraged by information technology. This implies that the information system strategy is a product or derivative of the command and control strategy. The information system strategy focuses on those management changes that achieve a significant return through the application of information technology and that are the results of the completion of the problem-solving process where the technology assessment is evaluated relative to the C2 needs. The second touch point of SIS and systems engineering comes during the implementation process as the project team is bringing out the new work way.

A side benefit to a gradual implementation of an information system change strategy is that the change can deal more effectively with incorporation of emerging technologies. This requires the technology assessment to account for the trends in technology developments and understand how these trends may benefit the long-term change roadmap of the military organizations.

Information technology supports this with both software (GroupWare, electronic mail, and relational databases) and hardware (networks and multimedia), the most exciting innovations being GroupWare and multimedia.

GroupWare and the new work way

The way that we work has changed ever since Xerox developed a capability for drawing people together on an on-line network to share information.[8] Networks first provided access for individual workers to share data and software with their local staff. Networking also increased the access of experts to information and to other problem solvers. However, there was still a boundary-individuals had to work as individuals and then merge their completed work together into a final product. GroupWare allows workgroups to cross that boundary and increase the efficiency of their shared problem-solving assets by allowing these individuals to work together in the same logical space on the computer. Because the computer has become the workplace, GroupWare allows the virtual operation of workgroup - members may be in various geographic locations and yet still share their thoughts and build their documents in a common, logical environment. Like electronic mail (Internet/ Intranet), GroupWare disrupts organizational hierarchies by permitting people to communicate with others outside their local organization. However, GroupWare differs from e-mail (Internet) in that e-mail permits one-to-one or one-to-many types of communication while GroupWare permits many-to-many communications.

The most popular type of GroupWare is represented by a single product, Lotus Notes®. It combines a sophisticated messaging system with databases of work records, memoranda, and electronic documents. It changes the way that information and documents are managed in an organization. Notes® operates under a different principle for communication responsibility than does e-mail. With e-mail, the sender of the message must identify all of the individuals who need the information contained in the message. With Lotus Notes®, the sender of the message forwards the message to a topical bulletin board, and anyone who needs information regarding that specific topic can access the bulletin board and read what associates are thinking and doing.

One report on this subject regarding the work of the staff concluded that GroupWare may be an unavoidable information processing improvement. Since GroupWare can increase the "mind share" of the corporate knowledge worker by sharing the same logical space with coworkers in a real-time operating environment**,** it can provide a tremendous advantage over the more linear systems used for document processing today. This equates to improvements in white-collar productivity through both cycle time reduction and increased performance through better communication.

Some of the most significant advantages listed in the report are:

- GroupWare changes the way the staff works.
- Greater access to information means that the workers must take more responsibility to access the information and to contribute to the ongoing dialogs and activities on the bulletin boards that define their work.
- GroupWare is most adaptable to a staff that has flexible cultures. Management has developed the philosophy that a decision improved and modified by group contribution is the desired outcome rather than one that may be

branded as the contribution of a staff officer. There is a tendency to use GroupWare as a social bulletin board rather than as work bulletin board.

One barrier to the implementation of GroupWare is the experience that many officers have with "junk E-mail" that has to be read. For instance at one direction of MoD, a worker would get between 5 and 20 electronic messages a day. This would be in addition to the 10 to 30 telephone calls, not to mention the 5 to 20 "hard copy" mails. One thing the managers fear is that the situation only gets worse with the advent of GroupWare, which exponentially expands the available information. One way around this dilemma, however, is agent technology.

Agent technology acts like an executive secretary to help workers filter and sort through information in bulletin boards and computer files to find exactly what they need. It uses artificial intelligence and hypertext-like capabilities to identify and alert their "principal" to the presence of interesting mail.

GroupWare enables the administration to develop wholly new structures where the team is the basic building block, and the need for cross-functional knowledge and rapid response to staff demands moves organizations away from fixed hierarchies and the organization matrix. These types of teams focus on assigned objectives that require innovative solutions. Such teams operate under disciplined processes that drive for the completion of their task. Teams in this mode operate together for a period of time and then dissolve as soon as the project is completed. Examples of this phenomenon already exist in Research & Development project teams, proposal generation teams, and "tiger" teams that are charted to fix a particularly perplexing problem. GroupWare helps to encourage the transition to these teams by breaking down functional barriers through an expanded access to "function-specific" information that is not allowed into the organization's common databases; creating a need for a shared language in order to communicate more effectively across functional boundaries; and providing the technical infrastructure that permits unit-staffs wide dialogue.[9]

Conclusion

The most important direction in enhancing the processes of command and control is the use of contemporary decision-making methodology. The environment for the information support of the management becomes crucial for success. The solution of these problems needs clearly and precisely defined management model, sound Information Strategy, and suitable organizational and technological tools. The GroupWare and the new information technologies will lead to the consolidation of all staff functions and the development of a new type of professionals, particularly in the field of strategic planning, research, and information systems.

Notes:

1. Velizar Shalamanov, “Problems of Information Security and Life Cycle Support of the Information Environment,” in *Proceedings of the 1996 AFCEA Sofia Seminar* (Sofia: AFCEA-Sofia, 1996), pp. 22-28.
2. Yantsislav Yanakiev, *Military Co-operation in South-Eastern Europe and the Future of Multinational Peace Support Operations* (Rome: NATO Defence College, Spring 2000).
3. Kaster, J., A. Kaster, *Componentware Approaches in Management Information Systems*, HFM Workshop (The Hague: 2000).
4. Gregory H. Watson, *Business Systems Engineering, Managing breakthrough changes for productivity and profit* (John Wiley, 1994).
5. Andriole, S. and Hopple, G., *Inference-Making and Option Selection in Army Corps-Level Tactical Planing: Some Hybrid Models and System Concept Storyboard* (Marsdhall, VA: International Information Systems, 1987).
6. Andriole, S., *Information System Design Principles for the 90s* (Fairfax, Virginia: AFCEA International Press, 1990).
7. McNurlin, B., R. Sprague Jr., *Information Systems Management in Practice* (Prentice-Hall, 1989).
8. Just as Xerox developed the WIMP or “windows-icon-mouse-pointing” computer environment, the personal computer, and object-oriented programming, the Xerox engineers also developed Ethernet as a means for connecting individual workstations together.
9. Carmel E. and J. George, “Joint Application Development (JAD) and Electronic Meeting Systems (EMS): Opportunities for the Future,” Working Paper CMI WPS 91-06 (University of Arizona, Center for the Management of Information, 1991).

JULIANA KARAKANEVA is born in 1953. She hold a M.Sc. degree in Automatics and Telemechanics from the Technical University of Sofia (1976), Ph.D. degree from the Technical University of Sofia (1983) with dissertation on “Methods for Logical Design of Fail -Safe Automatic Devices for Railway Transport”. Assistance-professor at the Military Research Development Institute of General Staff of Bulgarian Armed Forces, currently - Defense Advanced Research Institute, "G.S.Rakovski" National Defense College. Main research interests and activities: modeling and simulations, design of command and control systems, computer assisted exercises. E - mail: ju_karakaneva@md.government.bg.

GEORGY PAVLOV is born in 1951. He hold a M.Sc. degree in Automatics and Telemechanics from the Technical University of Sofia (1974), Ph.D. degree from the Technical University of Sofia (1979) with dissertation on “Automatic Control Algorithms for Stochastic Objects”. Associate-professor of Design & Development Information systems at the Military Research Development Institute of General Staff of Bulgarian Armed Forces, currently - Defense Advanced Research Institute, "G.S.Rakovski" National Defense College. Main research interests and activities, design of command and control systems, information systems, modeling and simulations. E - mail: gpavlov@md.government.bg.

BACK TO TOP

Advanced Technologies for Defense Information System Support

Yuliana Karakaneva and Georgy Pavlov

Keywords: Command and control technologies, information quality, GroupWare, networking, IT management.

Abstract: This article describes requirements of modern command and control of armed forces and some opportunities provided by advanced information technologies. The focus is on technologies for administrative support and management, with particular emphasis on GroupWare software and systems. The authors study the relation between scientists, software engineers and users in development and implementation of such technologies.

full text

Author: **Atanas Nachev**
Title: **Testbed for implementation of advanced IT Participation**
Year of issuance: **2001**
Issue: **Information & Security. Volume 6, 2001, pages 132-137**
Hard copy: **ISSN 1311-1493**

TESTBED FOR IMPLEMENTATION OF ADVANCED IT

Atanas NACHEV

Nowadays the quality and quantity of information resources are becoming important indicators of defense potential. Success in any type of military confrontation depends to a considerable extent on the results of the information confrontation between the opponents. When the combat potentials are comparable, reaching supremacy over the enemy is possible only through ensuring superiority in C2 systems, which these days cannot be realized without using the latest achievements in the field of information technologies. The development of C2 systems [1] is therefore considered to be the fastest and economically justified way to enhance the combat potential of the defense forces.

For defense purposes, advanced information technologies are materialized in different in purpose, range and realized functions automated management systems (AMS) and automated information systems. At operational and tactical levels, automation management systems may be classified according to purpose, structure and tasks. Each system of this kind is designed in modules, unified according to the specific functions it has to fulfill. The practical realization of such systems is accompanied by a number of difficulties, defined by factors such as diversity of troop units, distribution in space, expedition of the management activities and work in extreme conditions such as fire or radio-electronic influence by the enemy. The management automation of the troops' everyday activities is based on advanced information technologies. The characteristics in this case are as follows:

- Establishing favorable conditions to make general decisions by using common customer resources;
- Data processing and storing in the most convenient for the system location while meeting the necessary requirements for information security;
- Utilizing existing standards as the basis for integration within the system's framework and at an intersystem level;
- Modular design;
- Maximum use of existing equipment, even if it is not a subject of upgrading.

The systematic architectures being built are multilevel with vertical and horizontal branches.

Automated weapon control systems, the means for technical reconnaissance and radio-electronic warfare make up a special class of AMS with important problems to solve and a specific way of building and functioning, as a rule, in extreme conditions.

Activities directly connected with combat, operational and mobilization training of troops, as well as those potentially enhancing the effectiveness of field control systems, of armament and combat equipment have priority in automation. The role of the automated control systems and automated information systems used in staff work, especially for implementation of critical procedures, has increased. A promising approach to increase the stability and effectiveness of the control is the integration of resources for communication and control over troops and weapons.

The modern force management system is a complex multifunctional organism. Its effectiveness directly affects the successful fulfillment of the forces' functions. Nowadays, it is unthinkable to ensure effective management of troops and weapons without the overall utilization of the latest information technologies. That is why the "informatization" of the army should be approached as a priority task for the development of the armed forces. [2] It should also be accompanied by a clearly expressed governmental support, an appropriate defense budget structure, an overall scientific provision with the increased role of the military research units in the defense organization, [3] and a unified control over the processes of development and implementation of modern information technologies in the military area. Military research in this case should be viewed as an inseparable element of the general cycle of development, implementation and exploitation of resources and army management automation systems, carried out following a common plot and a unified management. This is a basic requirement for ensuring an overall and balanced automation of management processes. The experience so far has shown that any other approach leads to generation of irrational decisions, especially dangerous of which are those related to information security, [4] unjustified expenditures, corruption of the idea of increasing the combat capabilities of the armed forces through implementing modern information technologies.

It should be underlined that in the last thirty years a great number of different automated systems for troops and weapons management have been developed and implemented in the Bulgarian armed forces. Experience has been gained in the area of automation management of specific army conditions. Well-qualified scientific specialists have been trained and traditions in this field have been established. The development of information technologies in the 90s has put forward new challenges to upgrade the defense management systems in order to achieve fast, stable, reliable, continuous and flexible management of the armed forces in everyday and combat command. This calls for:

- Computer equipment in all management bodies, as well as in strategic, operational and tactical units;
- Complex automation of the everyday management of the armed forces and processes of control over troops in combat;
- Provision of a developed communication system, which allows prompt and reliable transmission of information with the necessary quality.

All this imposes a new approach to implementing new information technologies in the armed forces

management. The essence of this approach is in compliance with the following basic principles:

- All-round scientific support with maximum application of the available experience in the area;
- Profound research studies in military research units on specific defense problems, for which no ready-made decisions have been offered, and which, due to their specificity, have not been studied in civilian scientific organizations;
- Establishment of conditions for the research of proposed commercial-off-the-shelf solutions and justification of their applicability in the military area;
- Wide application of simulation and physical modeling of structural and functional solutions related to automation systems created for defense purposes;
- Certifying equipment and software according to their applicability in the defense area;
- Timely and effective training of personnel.

Following these objectives, the leadership of the Bulgarian Ministry of Defense designed and implemented a technological scheme for the development and implementation of defense information technologies, which meets the requirements listed above. It has been materialized in a specially built Research and Demonstration Center (RDC) in the Institute for Advanced Defense Research (IADR) at the “Rakovski” Defense College in Sofia. The RDC has been established to perform the following functions:

- Research on advanced technological solutions in the field of information and communications technologies with regard to their application in the army;
- Development and experimentation with software and technical applications designed specifically for the needs of the military;
- Testing of software-technical complexes and systems for management automation;
- Developing, experimenting and assessing concepts and means for information security;
- Physical modeling, simulation and study of advanced communications and information systems;
- Studying and certifying technical products for automation and systemic, technological and applied software;
- Training of personnel.

With its purpose, functions and establishment, the RDC has no equivalent in the country. Research is accompanied by the following specific features: conducting research on specific, essential for the defense of the country, scientific problems; creating necessary conditions to study proposed COTS technologies and solutions; creating functional models of systems under development; training personnel to use the systems being developed until they are in exploitation, using already built physical models of the systems.

For training purposes, a Center for Training on Network Technologies, including CISCO academy has been established in the IADR. The training process is carried out in close cooperation with the CIS and Interoperability Department in the “Rakovski” Defense College.

Scientific research in IADR on problems related to the development of communications technologies for the armed forces is carried out in accordance with the Plan for Scientific Activities at the MoD in close interaction with the Defense Planning Directorate and the Armaments Policy Directorate of the Ministry of Defense and the Communications and Information Systems Directorate of the General Staff of the Bulgarian armed forces. The research follows existing tendencies in organizing scientific studies in conditions of information warfare.[5]

The RDC is structured as follows:

- Research and demonstration hall with testing sites to study and assess commercial-off-the-shelf solutions and to build physical models and systems;
- Internet network which is an element of the general network environment of the “Rakovski” Defense College;
- Network Technologies Training Center;
- Laboratory for network technologies and information security;
- Laboratory for electronic means and systems;
- Spectrometric laboratory;

A center for lectures, presentations and mass media conferences has also been established.

The activities carried out in the RDC are connected with the implementation of the several basic programs of the Ministry of Defense: the Membership Action Plan; upgrading the command, control, communications, surveillance, reconnaissance and information systems; decreasing military infrastructure; research and administration.

The establishment of the RDC has contributed to the achievement of the following:

- Conditions have been created to carry out research on advanced technological solutions in the area of information and communications technologies with regard to their application for the needs of the armed forces;
- Necessary technological conditions have been created for physical and simulation modeling of communications and information systems;
- Analyzing, assessing and implementing advanced network technologies for the needs of the defense;
- Certifying automation equipment, as well as systemic, technological and applied software;
- Conditions have been created to train specialists from the Bulgarian armed forces on the

problems of advanced information technologies.

We believe that due to its purpose, realized functions and establishment, the RDC is unique and vitally important to the Ministry of Defense, General Staff of the Bulgarian armed forces and the state administration of the Republic of Bulgaria.

Notes:

1. Velizar Shalamanov and Todor Tagarev, *Information Aspects of Security* (Sofia: ProCon, 1996).
2. Velizar Shalamanov, “Problems of security and maintenance of life cycle of information systems,” *Military Journal* 58, 6 (1996): 83-90.
3. See Stefan Hadjitodorov and Todor Tagarev, "Scientific Research and Development in NATO," *Military Journal* 107, no. 4 (2000): 81-90; Matey Lalov, “Organization of advance defense research in conditions of information war,” *Military Journal* 59, 4 (1997): 90-98.
4. Shalamanov and Tagarev, *Information Aspects.*
5. Lalov, “Organization of advance defense research.”

ATANAS IVANOV NACHEV is an Associate professor at the “G.S. Rakovski” Defense Academy in Sofia, Bulgaria. Since January 2000 he is Head of “C4I systems” Section of the Institute for Advanced Defense Research. Prior to this appointment, Dr. Nachev served as Head of Communications and Information Systems Section of the Military Research Institute of the General Staff of the Bulgarian Armed Forces. He holds a M.Sc. (1979) and Ph.D. (1985) degrees in Computer Science.

BACK TO TOP

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

Testbed for implementation of advanced IT Participation

Atanas Nachev

Keywords: Research and Demonstration Center, automated management system, C2 management, prototyping, defense R&D.

Abstract: The development of C4ISR systems, systems to automate command and control, and system for automation of administrative and force management have priority in the modernization of the Bulgarian defense establishment. This article describes the Bulgarian experience in the provision of scientific support and environment for evolutionary development and testing of advanced information and communications technologies for the needs of defense. A Research and Demonstration Center was created in the Institute for Advanced Defense Research Institute at the “Rakovski” Defense College in Sofia. The author describes the purpose, the structure and the initial experience in the work of the Research and Demonstration Center and claims that it is of vital importance for the Ministry of Defense, the Bulgarian armed forces and the state administration.

full text

Author: **Dobromir Totev and Bisserka Boudinova**
Title: **Information Support for Effective Resource Management**
Year of issuance: **2001**
Issue: **Information & Security. Volume 6, 2001, pages 138-150**
Hard copy: **ISSN 1311-1493**

INFORMATION SUPPORT FOR EFFECTIVE RESOURCE MANAGEMENT

Dobromir TOTEV and Bisserka BOUDINOVA

Table Of Contents:

Background

Bulgaria started a radical defense reform aimed at adapting the role of the military factor in the national security system and developing modern armed forces. The defense reform reflects national strategic priorities, changes in the regional security environment, and resource constraints. In this regard, of great importance is the development and implementation of the an adequate system for defense resource management in the Ministry of Defense and the armed forces for the achievement of long-term objectives under forecasted resource constraints.

Information on defense resources and development of a database are indispensable for the efficient functioning of the defense resource management system. A database in place allows studies and analyses of defense resources. The respective methodology for defense resource management can be built on specific analytic and modeling programs. The unimpeded information flow through a Planning, Programming and Budgeting System (PPBS) is of paramount importance for the efficient functioning, hence for successful implementation of the system. Procedures and means for automatic collection and updating the information will facilitate working processes and increase the level of information and analytic authenticity.

During 1999, the Bulgarian Ministry of Defense (MoD) developed two long-term strategic documents - the Military Doctrine [1] and the "Plan for the Organizational Structure and Development of the Ministry of Defense by the year 2004," [2] later approved respectively by the Parliament and the Government. A decision was taken to implement Plan 2004 on a program basis. A necessary step was the creation of an integrated planning system covering both program development in the Ministry of Defense and the armed forces and defense budgeting. The planning system allows objective, effective and transparent allocation of resources, which would enable reliable civilian control.

The process of defense planning is based on the notion of unity of purpose, approach, resources, and time. A Planning, Programming and Budgeting System (PPBS) is implemented to support the process of decision making and provides a mechanism for consensus-building in programming and budgeting through joint planning and analysis of military force structures in the Ministry of Defense, by the Government and the Parliament.

Information on defense resources and development of a database are indispensable for the efficient functioning of the defense resource management system. A database in place allows studies and analyses of defense resources. The respective methodology for defense resource management can be built on specific analytical and modeling software. The unimpeded

information flow through PPBS is of paramount importance for the efficient functioning, hence for successful implementation of the system. Procedures and means for automatic collection and updating the information will facilitate working processes and increase the level of information and analytic authenticity.

The establishment of a global database requires the development of an information system that gathers, organizes and analyzes input data. System analysis will be built at the final information level - allocating the resources for the short-term and long-term planned activities. The established global database lays the foundations for developing the main planning documents in the MoD such as the annual defense budget. The main purpose of the global information database is to provide assistance in monitoring the implementation of multi-year defense programs. It is not possible to organize correct reports, precise planning, prognosis and control without the automated information system.

The database created by the information system serves as foundation of the informational support for the DRMM (Defense Resource Management Model). DRMM is the leading instrument for strategic and operational analysis in the field of defense planning. The abovementioned analysis helped to develop PPBS.

DRMM is designed to be an analytical tool used by high-level military/civilian planners in the macro analysis of a given country's defense system. [3] The DRMM is a computer model based on US defense planning practices. DRMM integrates force capability and cost assessment data into a single model that compares various tradeoffs between different force structure alternatives. The model is designed so that planners can create and modify the model's fundamental characteristics of a force structure in order to include the structure itself, equipment levels, manning, peacetime training, wartime stockpiles, and financial management practices.

The model produces outputs, both tabular and graphic, that quantify a country's force capabilities that can then be compared to alternative force structures and against the capability of a notional opposing or comparative force. Moreover, the DRMM contains integrated force capability assessment and cost analysis modules that help to model the benefits of different force programs. The information provided by the model can assist defense managers in making informed decisions.

Implementation of PPBS in the Bulgarian Ministry of Defense

In implementation of the Military Doctrine and the "Plan for the Organizational Structure and Development of the Ministry of Defense by the year 2004," a team in the Ministry of Defense proposed the creation of an integrated planning system to allow for objective, effective and transparent allocation of resources, and to enable reliable civilian control.

The requirements towards the newly created system are as follows:

- To ensure a long-term binding of defense resources with defense/combat potential;
- To be compatible with the planning systems of NATO and NATO member countries;
- To lay the foundations for effective civilian control and transparency in the defense budget formulation in compliance with the requirements of the Bulgarian Military Doctrine.

Borrowing the name from the analogous US system, the planning system became known as PPBS. It adapts the principles of effective defense resource management to the traditions, organizational limitations and realities in Bulgaria. The creation of an integrated planning system adds to the effort of the Ministry of Defense to develop a defense system with force structure, doctrine, and equipment compatible with these of the NATO member countries.

The implementation of different PPBS levels results in a basic framework of the process of program and budget evaluation by the National Assembly (the Bulgarian single-chamber Parliament), society, allies and partners.

Practically, one of the main results of the PPBS is the development of a Six-Year Defense Program: an official document that comprises comprehensive information about the approved defense programs. It stores information for the previous year, the current year, the budget period and the next five years. It is necessary to maintain a computer database that is updated no less than four times a year as follows:

- During the annual review of implementation;

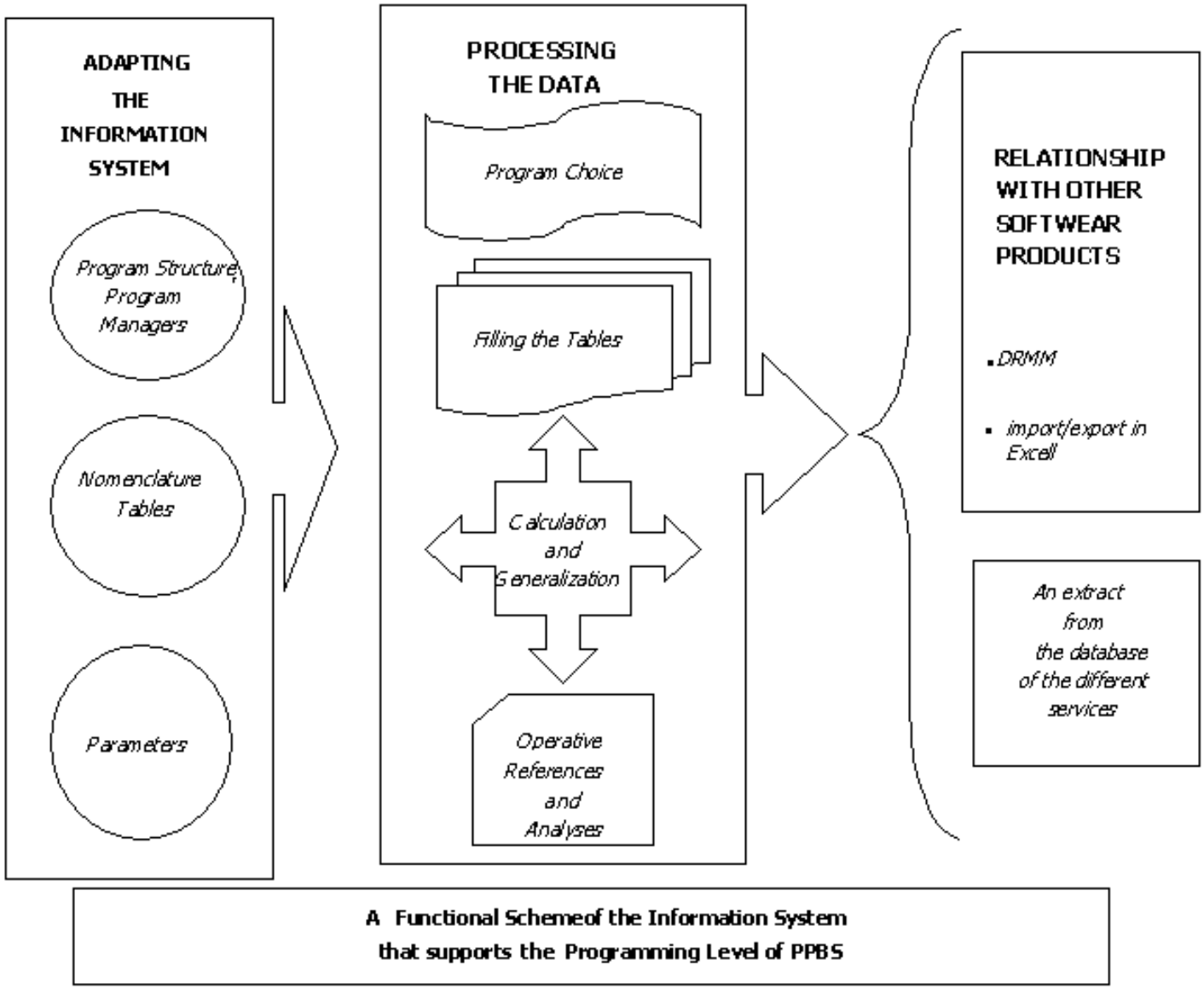
- During the presentation of the already developed program memoranda;
- During the budgeting process in MoD;
- After parliamentarian approval of the defense budget.

All related information is stored in a hierarchical database reflecting the structure of the defense programs.

Information support for PPBS

The establishment of a global database requires the development of an information system that gathers, organizes and analyzes input data. System analysis will be built at the final information level - allocating the resources for the short-term and long-term planned activities. The established global database lays the foundations for developing the main planning documents in the MoD such as the annual defense budget. The main purpose of the global information database (GID) is to provide assistance in monitoring the implementation of multi-year defense programs. It is not possible to organize correct reports, precise planning, forecasts and control without the automated information system GID. The principles of GID are presented in Figure 1.

Figure 1



A Functional Schemeof the Information System that supports the Programming Level of PPBS

MoD will test a prototype of the described GID in 2001. The prototype is developed using Microsoft Office ACCESS database software. The program modules are built using Visual Basic environment. The main program consists of normative

information - program structure, program managers, nomenclature tables (menus) and tables of the system parameters - an opportunity to choose the initial fiscal year and specific filters. The filters are set up depending on the survey level: MoD, General Staff of the Armed Forces (GS), or the services. The system will be adapted to operate not only at the level of major programs, but will incorporate their sub-levels: programs, sub-programs and program elements (see figure 3). One of system parameters allows choosing the variant of data we have in database - approved (planned in Programming Guidance) or active (current) variant of allocated resources by programs.

There is an option to work with a system of sub-level databases, i.e. for a single service or single program. This means every representative (program manager) from MoD, GS or services will have a limited information access to his working area. An extract database from global database will be created along the chain of command. For instance, there will be copied a separated database with concerning defense programs for the GS, for services - Land Forces, Air Forces, Navy. The next step is to generalize the input data from the sub-levels and to do calculations.

There is no limit for the number of subordination levels in the program structure. The system allows the attachment of new levels (programs) and the deletion of old ones. The database includes twelve complete tables for each program, sub-program or program element. For each program the number of the rows (nomenclatures) in the menu-tables could be different, as every program requires specific resources.

The nomenclature in menu-tables can be altered at the highest level of database access only. The tables “Resource allocation plan for program provision” and “Generalized Sample Table for concrete year from a Program Objective Memorandum” are program oriented. All other tables are connected with the resources allocation according to budget accounts. This structure allows the expenditures based on programs and budget accounts within every program to be followed. As a result, the defense budget could be built on a program or budget accounts basis.

The menu-tables are:

- Resource allocation plan for program provision;
- Draft budget account for necessary funds by programs;
- Planning table for reduced during reform personnel and financial funds for compensations;
- Plan - account for military exercises expenditures;
- Foreign currency payments planning table;
- Planning table for scholarships financial funds;
- A table for paragraph 18-00 “Other expenditures”;
- A table for paragraph 46-00 “Membership payments, participation in international non commercial organizations and other activities”;
- A table for paragraph 36-00 “Other non tax incomes”;
- A program for expenditures in building (repair) of military infrastructure;
- Generalized Abstract Table for concrete year from a Program Objective Memorandum.

The first step is to choose the period and then the respective database. This structure of software allows the storage of several databases, from different stages of the defense program development (programming, program review process, budgeting). The next step is to choose certain program (subprogram). After that it's necessary to input actual figures for the previous, current and budget year and the prognosis for the next six-year planning period.

The database allows the input of planned and actual figures. GID allows the development of a control system that covers the financial resources spent at any level of the program implementation. This means fourteen tables to be completed with the planned and actual figures. In case a new program is developed the data for the assets spent can be transferred in a database. This secures the control over the spent financial resources. Alternative variants should be created in the fields of financial and capital resources. The alternatives for each program are based on the already approved main PPBS documents - the PPBS Concept and Methodology for Program Development in the MoD. There is possibility to create alternatives with

various financial funding – 10 percent less or more than the financial quota for the program. The main purpose is to easily combine the required resources, namely number of units, employees, armaments and equipment, capital expenditures and their financial equivalent. Each alternative should be precisely evaluated in order the planned objectives to be accomplished. The evaluation process will result in the proper (optimal) alternative choice.

GID allows the verification of the resources for the main programs, sub-programs and program elements on annual basis. This results in a comparison between the planned resources and resources actually granted. The comparison should be made for each program for the current year or the whole planning period.

An interface for Excel connection was developed allowing information exchange with an Excel table. The connection assures Microsoft Office interoperability.

There is an opportunity for a strict control over the data, information protection and level access. The references that could be gathered enable a precise analysis of the information completeness for each program. This principle seriously reduces the risk of duplication of information.

The database created by the information system is the foundation of the informational support for the DRMM (Defense Resource Management Model). DRMM is the leading instrument for strategic and operative analysis in the field of defensive planning. The abovementioned analysis helped us to develop PPBS.

DRMM as main tool for analysis and modeling of defense resources

DRMM is designed to be an analytical tool used by high-level military/civilian planners in the macro analysis of a given country's defense system. [4] The DRMM is a computer model based on US defense planning practices. DRMM integrates force capability and cost assessment data into a single model that compares various tradeoffs between different force structure alternatives. The model is designed so that planners can create and modify the model fundamental characteristics of a force structure in order to include the organizational units, equipment levels, manning, level of personnel peacetime training, wartime stockpiles, and fiscal management practices.

The model produces outputs, both tabular and graphic, that quantify a country's force capability that can then be compared to alternative force structures and against the capability of a notional opposing or comparative force. Moreover, the DRMM contains integrated force capability assessment and cost analysis modules that help to model the benefits of different force programs. The information provided by the model can assist defense managers in making informed decisions.

The DRMM is designed to assist governments with a computer model that will:

- Help civilian defense and military officials develop cost-constrained, cost-effective defense programs;
- Familiarize officials with the Planning, Programming and Budgeting System (PPBS) techniques and methodology;
- Provide military and civilian leaders with a national defense planning model;
- Help to balance national defense expenditures against economic and political reform efforts; and
- Assist countries in providing for their defense requirements during a period of (severely) constrained budgets.

The DRMM operates on any IBM-compatible personal computer in the Windows environment. Developed using the Microsoft Visual FoxPro database management system, the DRMM stores tens of thousands of data elements representing key characteristics of any given national military force structure.

Data Requirements

The DRMM is a deterministic data model consisting of four different types of data, namely force setup data, cost setup data, force (or unit) data and cost factors. Force setup data consists of qualitative information, such as the universal set of weapon types, war reserve material types, personnel types, and critical organizational unit characteristics to be used in the model. Force setup data also includes limited calculation factors such as the range of possible unit mobilization times. The setup data serves as the building blocks or reference lists of information that will be used to assign characteristics to specific units

or whole force structures and to include the Opposing Force/Comparison Force. Matching specific unit information with force setup data creates force (or unit) data.

Cost setup data defines country-specific currencies, cost accounts, budget categories, project names, inflation factors, and unit types. The second level of data is the Cost Factors for personnel, equipment operating, unit operating, equipment procurement, and project costs. These can be defined as either “actual” cost based on historical pricing or “standard” costs from engineering or financially calculated standards. It is also at this level where funding factors can be applied to the individual cost factors. Inflation rates are also found at this level.

The model uses setup data to facilitate the user access to force data and cost factors. In the DRMM there will be only one combined force-cost body of setup data which remains constant for all alternative force structures modeled. Conversely, there will be as many combined sets of force (or unit) data and cost factors for each force structure alternative entered into the model. The differences are in the multiple Force and Cost data sets, particularly in quantity for uniquely defined alternatives. The following paragraphs will explain each of the four categories of data in detail.

The DRMM is used to store data, which represent the various key cost and force characteristics of a national military force structure. There are two major components of the DRMM: the force module and the cost module.

a. Force Module

Within the force module, the DRMM focuses on four major areas: units, equipment, personnel, and resources. These four areas are briefly described below.

(1). *Units*

The force structure is described at the unit level and at a level of detail determined by the user. Force and cost data can be reflected at the regiment and/or separate battalion level, whereas the organization of some countries Armed forces may dictate that force and cost data, is maintained at a lower echelon, e.g. company. In addition to describing a country’s own armed forces structure, an opposing force (threat)/comparison force structure can be developed to compare the relative combat capability of the two forces. In cases where the description of a realistic opposing force is too politically sensitive, this option can be used to measure regional parity between neighboring countries or a comparative notional force. This option of software allows the comparison of trends in combat capability between alternative force structures and is not intended to predict battle outcome. The model can generate a ‘buildup graph’ of selected forces, reflecting the readiness level, training time, and travel time under a defined scenario.

(2). *Equipment*

The equipment inventory of a country’s force structure and its associated activity level is entered in the DRMM at the major item of equipment level. The DRMM uses a weapon system scoring methodology that assigns a numerical value to the major combat systems (tanks, APCs, artillery, etc.) in the inventory. The combat power of a force is computed by aggregating the total weapon systems scores for all equipment in the selected unit inventory. This score represents a static measure of the combat capability of a force, and as long as this not a war game, it does not predict the outcome of a conflict. Although equipment, such as trucks and other non-firepower related items, should be entered in the model for costing and training purposes, these items of equipment do not receive a combat capability score. The model produces combat capability output in five different levels: Authorized, Actual, Mission Capable, Effective, and Training. The model also allows the user to show degraded combat capability due to reduced equipment on hand, equipment under repair, lack of training on equipment and lack of resources to fully use the equipment. The associated activity level of the equipment allows the model to calculate unit operating costs and a rough measure of unit training levels.

(3). *Personnel*

The DRMM accounts for personnel at the unit level. Personnel quantities are entered at the unit level based on Personnel Types. Personnel Types must be agreed on by both the force team members and the cost team

members so that personnel quantity data reflected at the unit level are compatible with the budget personnel accounts.

(4). *Resources*

The DRMM accounts for user-defined resources (sometimes called war reserve material) at the unit level. The types of resources included in the model are defined by the user in the Forces Setup files under Resource Types and Resources. Typically, ammunition and POL are two major resource types tracked in the DRMM but resource categories of spare parts, crews, food, etc. could also be defined. The required and actual quantities of a defined resource are entered in the DRMM at the unit level. The DRMM also includes a function to allocate resources from a higher level to a lower level (e.g. from brigade or depot to battalion if actual quantities exceed required quantities at the brigade level and a shortage of the same resource exists at the battalion level). Resource Types can also be categorized to cause a degradation in combat capability (the 'effective' score) in case there are resource deficiencies.

b. Cost Module

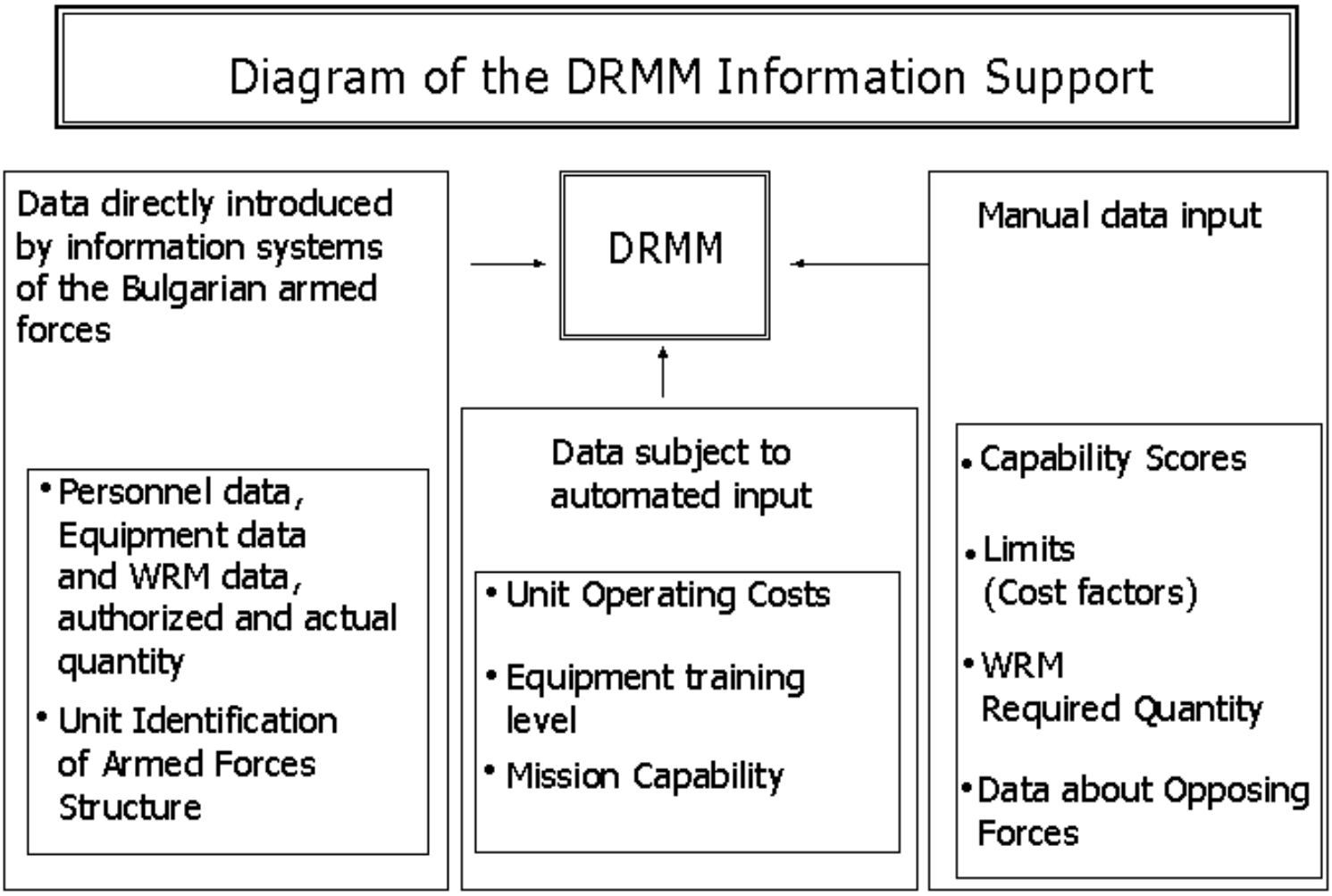
The cost module defines peacetime operating costs of a country's defense program in the four major areas of defense resource management: force structure costs; readiness costs; investment cots; and sustainability costs. The DRMM model also incorporates inflation rates so that these costs can be viewed in terms of their escalated values in future years. In practice, DRMM advocates a unit-based costing approach where the above mentioned costs are associated as much as possible to specific units. In this manner the DRMM approach builds the costs from the bottom-up as opposed to a top-down allocation approach historically used by many countries.

The DRMM costing approach is also one of decision "support" rather than decision "making". DRMM does not attempt to optimize resource allocation. Rather, DRMM allows the user to develop likely alternatives whose effect on costs can then be analyzed and evaluated. This approach facilitates the force and cost analysts to be more intimately involved in the modeling effort than one where the model dictates a solution.

DRMM may be provided with data manually and automatically. It is very important opportunity for a fast development of the database necessary for DRMM functions to be granted. The database should be often updated automatically because of the significant volume of information. The updating should be done using the already existing information systems.

The compatibility of the Model with the existing information systems, keeping force section (personnel, equipment, WRM etc.) and allowing transformation of these data to the DRMM system data, is very important for its functioning. This allows us to update the data easily and on time. The manual introduction of data is time consuming but it can eliminate the risks of errors to a great extent. **Figure 2** presents the diagram of information support that was tested in the Bulgarian Ministry of Defense.

Figure 2



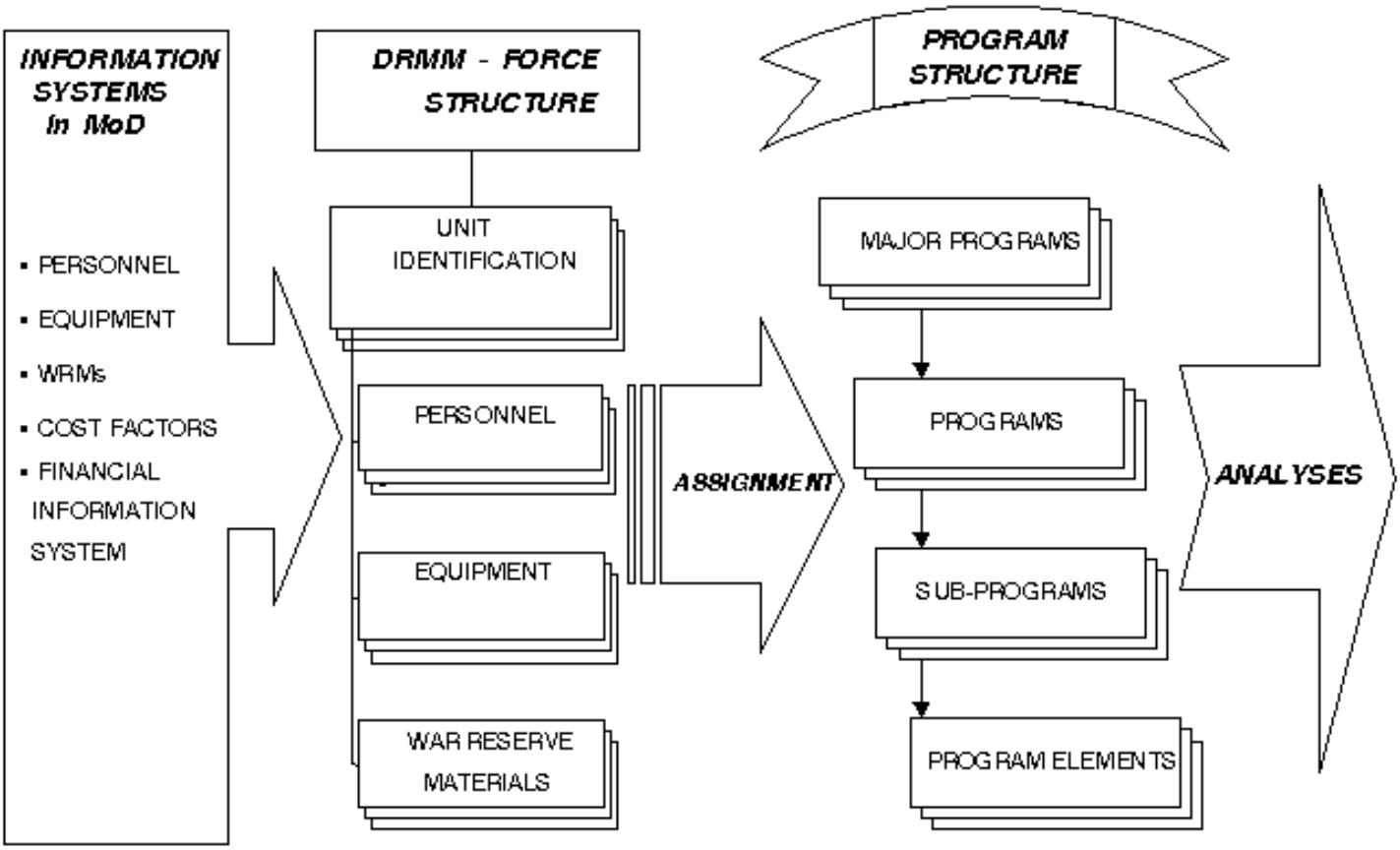
The functional scheme of the connection between the organizational structure of DRMM and the hierarchic program structure of the MoD is depicted in Figure 3. The newest version of DRMM enables data relation between DRMM and PPBS. The program relation allows a serious enlargement of the analysis spectrum.

Conclusion

The DRMM informational base is indispensable for the proper functioning of the system. The process of automatic gathering and updating of the information will disencumber the working environment and increase the level of information authenticity. It is crucial that the planning management prepares clear global and factual initial cases for the development of information systems supporting PPBS. Analytical tools, such as DRMM, will improve the planning, programming and budgeting processes.

Despite the huge amount of difficulties related to the execution of the objectives of the new Bulgarian Military Doctrine, Plan for Organizational Structure and Development of the MoD by the year 2004, and the implementation of PPBS in MoD, the process of reforms is irrevocable. It will provide a missing link in the civilian control in the Bulgarian Armed Forces, thus contributing to Bulgaria's preparation for NATO membership.[5]

Figure 3



Notes:

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. *Plan for Organizational Development of the Ministry of Defense till 2004* (Sofia, MoD, 1999).
3. *Defense Resource Management Model, User's Manual*, Department of Defense, US, 1998.
4. Jones, L.R. and Bixler, G.C., *Mission Financing to Realign National Defense* (Greenwich, Connecticut: JAI Press, 1992).
5. Todor D. Tagarev, "The Missing Link in Civilian Control," in *Proceedings of the MAP Seminar on Regional Cooperation in Enhancing Civilian Expertise and the Role of Civil Society in Security and Defence Policy Making* (Sofia: February 2000).

DOBROMIR TOTEV TOTEV (b. 1957) is Chief of Department in "Defense Planning Directorate", Bulgarian Ministry of Defense. Colonel in the Air Force, M.Sc. in Radar & Automatics (1980), "Rakovski" Defense College (1991), Defense Resource Management Course (DRMI – Monterey, USA, 1999). Currently, Colonel Totev is student at the NATO Defence College in Rome, Italy. *E-mail*: D.Totev@md.government.bg.

BISSERKA LYUBENOVA BOUDINOVA (b. 1963) is Chief of Section in "Defense Planning Directorate", Bulgarian Ministry of Defense, M.Sc. in Mathematics (1986) - Sofia University, Defense Resource Management Course (DRMI –Monterey, USA, 2000). *E-mail*: B.Boudinova@md.government.bg.

BACK TO TOP

Information Support for Effective Resource Management

Dobromir Totev and Bisserka Boudinova

Keywords: Programming, Integrated planning system, Transparency, Defense Resource Management Model (DRMM), deterministic computer model, program structure, Force Module, Cost Module.

Abstract: Defense planning is a complex process that accounts for qualitative factors such as changes in security environment and political priorities, and quantitative factors such as costs, resource constraints and various measures of capabilities and risks. This article describes the Bulgarian experience in implementing advanced information technologies to support the process of defense planning, including phases of long-term planning, programming, and budgeting. The focus is on the implementation of the Defense Resource Management Model (DRMM) to match required capabilities and available resources during the programming phase.

full text

Author: **Information & Security**
Title: **C4 Common Technical Architecture Development Coordination Group**
Year of issuance: **2001**
Issue: **Information & Security. Volume 6, 2001, pages 153-156**
Hard copy: **ISSN 1311-1493**

C4 COMMON TECHNICAL ARCHITECTURE DEVELOPMENT COORDINATION GROUP

CONCEPT FOR ESTABLISHMENT WITHIN THE SEDM [1] PROCESS

Table Of Contents:

I. Purpose

The occurrence of various crises and natural disasters on the Balkans in the past few years strongly supports the need to create a multinational coalition environment for exchange of information among regional partners. For successful implementation of this idea it is necessary to combine information management capabilities of the present and future common regional structures and systems and nationally provided capabilities, i.e., to establish a common technical architecture framework for information management. Another dimension of cooperation in the C4ISR [2] area is added after September 11, 2001, and the evolving global antiterrorist coalition.

The C4ISR systems studies, conducted recently in most PfP countries in the region, identified similar problems in the field of communications and information systems (CIS) and the plans for their modernization. In order to ensure, in a cost-effective manner, interoperability among the CIS systems of different countries, as well as interoperability with the NATO CIS, the process of modernization should follow a strictly determined technical architecture. On the other hand, a number of present and future SEDM initiatives imply or explicitly require the existence of such common regional architecture. The need to ensure the interoperability among the national and SEDM-common systems calls for a coordination of the process of determination and upgrading of this technical framework. This process is further complicated by the fact that modern communication and information technologies develop extremely fast.

The modernization of the C4ISR infrastructure is a challenge from acquisition and procurement point

of view, with important requirements in the area of Research and Development (R&D) and Education and Training (E&T), as well as in terms of participation of national defense industries and academic sector in the upcoming and current projects. National content is essential for C4ISR systems, especially regarding software. Thus, a balance between national and international efforts, partnership between public, private sector and NGOs, including the academic sector, will be essential.

One of the possible approaches to solve these complex problems is the establishment of a *C4 Common Technical Architecture Development Coordination Group* [3] within the SEDM process. The group has to comprise experts in developing C4 systems from the SEDM countries. At regular working meetings the C4 Coordination Group will discuss and propose for approval solutions to problems in the following fields:

1. Definition of technical architecture of technologies, standards, protocols, interfaces, data formats and procedures for data management within which to develop present and future SEDM C4 systems and to insure their functionality in the regional communications and information infrastructure, that is still heterogeneous.

2. Development of a strategy for improvement and further expansion of the shared usage of common systems within SEDM, such as PIMS, CIN, SEESIM.

3. Development of an integral mechanism for analysis and assessment of the C4 systems interoperability - lessons learned from PfP exercises - and creation of a shared database.

4. Coordination, if necessary, on bilateral and multilateral bases of the issues, related to the exchange of information and the interoperability of common projects and systems.

5. Study of possibilities for shared use of the centers, built in different countries, for testing C4 systems interoperability, as well as centers for research and demonstration of advanced technologies. Creation of a proper mechanism for exchange of information on conducted tests and studies of hardware and software.

6. Establishment of a new type of partnership between local industries, Ministries of Defense and international C4ISR companies in the areas of procurement, R&D, E&T, and a strategy for coordinated efforts in restructuring of defense industries, privatization and procurement.

7. Establishment of a new role for NGOs and academic institutions for higher transparency and efficiency in the use of modern IT, especially dual-use, commercial-of-the-shelf, state-of-the-art equipment, and in mechanisms for outsourcing IT services.

II. Scope & Functional Areas

The scope of the C4 Coordination Group will cover, but is not limited to the following functional areas:

1. User Interface
    a. UI Services
    b. HCI
    c. Graphics & symbology
    d. VTCs
2. Information processing services
    a. Operating Systems
    b. Internationalization
    c. COP/GIS/Terrain visualization
    d. CAX and M&S issues
    e. CBT/Online Training/Distance Learning Systems
    f. Data Management Services
3. Communications
    a. Communications Services
    b. Communications Components
    c. LAN/WAN
    d. External Interfaces
4. Information Interchange
    a. Document Data Interchange
    b. Graphic Information Interchange
    c. Multimedia Interchange

d. Messaging

e. Web based Information distribution & Applications

f. Tactical Data Link Processing

g. Collaborative Technologies & Tools

5. Networks (Systems) Management

a. Monitoring of status

b. Addresses management policy

c. Fault recovery

d. Topology controlling

6. CommSec / InfoSec

a. Equipment

b. Software

c. Interfaces

d. Procedures

7. Legal and organizational issues

a. Institution of CIO in SEEDM countries

b. Development of Program Offices, Test-bed Centers, Operators for C4ISR infrastructure in Government

c. Development of software development centers, maintenance centers, R&D centers, E&T centers outside Government around main defense contractors

d. Institutionalization of joint procurement for the region

III. Structure and Organization

It is appropriate that the C4 Coordination Group includes representatives of Ministries of Defense of all countries participating in the SEDM process, as well as in Multinational Peace Force in South East Europe (MPFSEE), while preserving the open format of the organization. The Group shall perform its functions as a military-technical expert body supporting the SEDM Coordinating Committee in the field of C4 system development.

It is possible to launch officially the C4 Coordination Group at the Second Regional C4ISR Conference "Systems integration and Program Management" during the HEMUS 2002 defense exhibition in Plovdiv, Bulgaria, in May 2002. This can be truly joint event with participation of Ministries of Defense, industries, academics, and NGOs. A set of demonstration of C4ISR solutions can be arranged during "HEMUS 2002," related to the activity of MPFSEE and using Bulgarian military facilities.

***Points of contact*:**

Bulgarian Academy of Sciences:
Dr. Velizar Shalamanov, *E-mail*: bon@mbox.digsys.bg

Ministry of Defense:
LTC Nikolay Petrov, *E-mail*: petrovn@bg.pims.org

Notes:

1. SEDM – South-eastern Europe Defense Ministerial (process).
2. C4ISR – Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (systems)
3. Further – “C4 Coordination Group.”

BACK TO TOP

Author: **Information & Security**
Title: **SEEDEFCOL - Virtual Defence College for Distance Learning in South East Europe**
Year of issuance: **2001**
Issue: **Information & Security. Volume 6, 2001, pages 157-166**
Hard copy: **ISSN 1311-1493**

SEEDEFCOL - VIRTUAL DEFENCE COLLEGE FOR DISTANCE LEARNING IN SOUTH EAST EUROPE

VISION FROM BULGARIA

Table Of Contents:

The Concept

Security Context

The logic of the stabilization of the South East Europe (SEE) requires a complex approach for achieving lasting peace, stability and security in the region. There is no doubt that the way out of the entire situation is exclusively through political, economic and security cooperation. The promotion of transparency and mutual confidence in defence and security related issues are between the key tracks that lay at the basis of the regional military cooperation and partnership for peace.

Armed forced and defence establishments remain important factors in this process. During the last

decade, they faced challenges that deeply effected the basics of the traditional strategic culture: rethinking of the age-old vision about the army as the only guardian of the nation, radical reengineering of all defence system, implementation of European type civil-military relations and democratic oversight, reformulation of the old and new military professional values, modernisation of the existing military art through application of NATO standards and procedures.

The countries from the region that cooperate in the Euro-Atlantic format make significant and systematic efforts to accomplish real progress in the interoperability, implementation of an effective democratic oversight of the military activities and full modernisation of the existing system of military education and training. There is shared understanding that success in the coming years will depend to a great extent on the reform in the way of teaching and training military professionals.

People's knowledge and skills are the target. "Struggle for human resources" is the motto of ongoing defence reforms. "How to build non-traditional military leaders now?" is the core question of tomorrow's democratic Balkans. The education and training are the shortest way to the new military professionalism, interoperability and integration. The transparent cooperation in defence education and research can contribute to the mutual confidence across the region.

Collaboration and encouragement of all SEDM[1]-based initiatives for sustainable military cooperation have been at the forefront of Bulgarian foreign and security policy. That is one of the national priorities within the Consortium of Defence Academies and Security Studies Institutes (called further *Consortium*). It supplements Bulgarian commitment in related areas as The Stability Pact for SEE (*Working Table No. 3*), SEEBRIG and BLACKSEAFOR.

For that purpose, the initiative to establish *Virtual Defence College for Distance Learning in South East Europe (SEEDEFCOL)* was lunched during the Third annual conference of the Consortium in Moscow, Russia, 25-27 June 2001.

Vision

The idea is based on the long-range vision of NATO Partnership for Peace to create a distributed environment in which all nations, including their universities and academies, have an equal opportunity to develop, deliver, and manage learning tools and course content. All of these efforts are designed to harmonize and greatly enhance military and defence related education and training at all levels.

Efforts to develop regional architecture and operational environment of the C4 systems on the basis of *Partnership for Peace Information Management System* (PIMS) in South Eastern Europe will create sufficient foundation to establish SEEDEFCOL.

Additionally, with the development of exchange programs, SEEDEFCOL will facilitate the conduct of collaborative research and development by expert from various countries.

This project will improve the capabilities of the countries in SEE region to contribute substantially to the enhancement of peace and security not only in the Balkans, but also throughout Europe.

Functionally, the virtual College could combine existing expertise in different fields and existing Centres of Excellence in the SEE. The organizational environment could be the *Consortium of Defence Academies and Security Studies Institutes* and also the *Southeast European Defence Ministerial* process and mechanisms. The College will communicate with the NATO *Training and Education Enhanced Program* (TEEP) and will become a substantial component of the *On-line Defence University*. Such kind of integration will accommodate many different nations with many different and specific training, education and research needs. It will provide good conditions for effective transfer of interoperability know-how and will stimulate standardisation in defence education and training for more multinational capabilities. (See *Model for Euro-Atlantic military education and training*)

Aim and Objectives

The College is primary aimed to promote cooperation between defence research and education institutions from the countries of South East Europe and also among *centres of excellence* studying security and defence related issues.

The core objective of the College is to support international efforts in regional and EAPC [2] format to promote defence reforms through enhanced application of information technologies in military education, research and training. In a triple approach, it intends to:

- Provide high quality research and training, tailored to the requirements for interoperability and integration and reduce time and cost of developing and distributing defence and security data, information and analyses and related advanced training modules;
- Utilise common with NATO countries standards in research and training that will provide cost-effectiveness durability and flexibility of the interoperability efforts.
- Encourage widespread cooperation in developing and sharing of research and learning resources across the region (and within PfP boundaries) and contribute to enhancement of mutual confidence and stability through transparency and collaboration.

Activities

SEEDEFCOL activities should be issue-driven. The SEEDEFCOL members and partners will establish a process for accelerating implementation of next generation technologies in the region in order to bridge the gap from research and development to learning and implementation. To this purpose initially, the College could focus on:

- Joint studies in advanced defence resource management;
- Searching for and providing information and access to good practices in defence management, interoperability improvements and civil-military relations;
- Joint production and electronic delivery of materials related to transparency in defence and armed forces;

- Development and exchange of ADL [3] training modules and packages;
- Exchange and joint use of data, information and analyses;
- Joint training and exchange of experts, researchers, trainers and lecturers;
- Teaming of experts and trainers;
- Exchange of training and testing packages related to the nationally approved Partnership Goals;
- Support to the Stability Pact for SEE, Working Table No.3 activities.

SEEDEFCOL activities shall be carried out through various instruments to deliver effectively useful products as follows:

- *Assistance*: The College shall generate programs for education, training and research addressed to the needs of the member countries and also to assist their execution on national and multinational bases.
- *Networking*: In order to perform the role of a "clearing house," the College shall establish and engage in networking of researchers and practitioners that are dealing with ADL-based education and training modules and research data.
- *Documentation*: The College shall establish a powerful documentation IT-based capabilities. In close cooperation with the Consortium WG, George C. Marshall Center and NATO units, it will develop a virtual library for mutual reference use.
- *Consultancy*: The College has to establish relations with distinguished and experienced institutions that could provide consultancy to the member institution in preparing and using ADL-based opportunities.
- *Feedback and Lessons Learned*: The College shall establish a feedback mechanism, which will provide realistic evaluation and lessons learned for all the member institutions.

Functional Environment

Along the model of the Consortium of Defence Academies and Security Studies Institutes, the Conference of the Commandants, the Conference of the PfP Training Centres and Simulation Network, SEEDEFCOL should be *association of the willing* among the defence education, training and research institutions and *centres of excellence* from the EAPC countries from South East Europe. (See *South East European defence college network*)

The principal "political shoulder" of the College could be *The Southeast European Defence Ministerial (SEDM).* It has been created as a forum for consultations and joint planning, firmly bound to the Euroatlantic integration of the region. It shows the will of the participating states to share and act in conformity with common values and principles. Thus, the proper institutionalisation of the cooperation throughout the region is essential for the promotion of stability and security.

The regional environment for the College could be the Pact of Stability for SEE, the Crisis Response Information Network (CRIN) and the South East Europe Simulation Network (SEESIM) that are potentially both contributors to and beneficents from the SEEDEFCOL activities.

> *The Stability Pact for SEE* makes efforts focused on different programs for re-qualification and social adaptation of discharged military personnel, confidence building measures, increasing transparency in military sphere, effective management of the defence resources, mine clearance issues, control of arms trade and prevention of illegal traffic, etc.
>
> *A regional Crisis Response Information Network* (CRIN) is in process of establishment. It will ensure fast information exchange, operability and possibility to coordinate the activities of each country in the region during disasters and crises.
>
> *South East Europe Simulation Network* (SEESIM) has been planned to function within the regional context in a way similar to the network demonstrated at the NATO Washington Summit in 1999. It is intended to assist the SEDM countries to establish integrated operational capabilities and reach an average level of interoperability with NATO member states in terms of communications systems.

The strategic environment of the College could be the *NATO Training and Education Enhanced Program (TEEP).* All six elements of the program are fully applicable to the purposes of the College. TEEP can also benefit from our efforts because national contribution is essential both for SEEDEFCOL and TEEP.

> *The consortium of twelve* NATO Partnership for Peace nations that work with the ADL Co-Laboratory in Alexandria, USA, could also provide "open source" learning and research management system that is consistent with the specific of SEEDEFCOL.

The initial *organizational environment* could be the *Information Technology Working Group* of the Consortium of Defence Academies and Security Studies Institutes.

> SEEDEFCOL concept is fully compliant with the idea of **t**he PfP Consortium of Defence Academies and Security Studies Institutes. The College can co-operate with and benefit from all the Working groups. The Consortium partner and member institutions can also contribute to development of an initial concept and related infrastructure. The efforts of the Consortium to develop learning management system software can be provided to the regional countries at no cost. It will enable each of our educational and research bodies to develop and distribute databases and ADL courses that are interoperable and reusable across the region.

The *three technological pillars* of the College are:

a. INTERNET, as standard working environment, and PIMS as provider of access;

b. Advanced computers as research and learning (multi-media) workstations; and

c. Local Intranet (LAN) upgraded at the level of ATM advanced communications systems with increased bandwidth and quality of delivery.

PIMS is the perfect communications environment for the College. Established practice and infrastructure with the support of PIMS experts could be organized in order to facilitate the collective efforts of SEE countries.

The College also could attract the attention of distinguish defence universities, institutes and also big companies that produce advanced distributed learning modules and packages, information and communications assets and technologies for distance learning.

Initial Organization

The initial organization of the College could include:

- Interim *Director of the College*, selected by the SEDM ministers of defence;
- Hosting institution that will provide SEEDEFCOL *Secretariat* for mission support and administration, *IT manager* with small staff that will manage the documentation and the website of the College;
- *International Advisory Board* chaired by the Director could consists of directors of member and partner institutions, as well as officials from NATO who manage the TEEP Program;
- *International Board of Experts* that will draft the annual and perspective programmes of the College and will manage their execution.
- *Each member institution* will continue in its individuality, but each could also contribute to the College objectives and through them – to the On-line Defence University, Euro-Atlantic Defence University, Euro-Atlantic Education Programs and Euro-Atlantic Education and Training Network, as they were presented by Ms. Lisa Bronson (Deputy Assistant Secretary of Defence for European and NATO Affairs, US) during the Third Annual Conference of the Consortium of Defence Academies and Security Studies Institutes in Tallinn, Estonia, in the year 2000.

Expected Results

The immediate benefit of SEEDEFCOL will be:

- to stimulate the reform in military education and research systems introducing advanced methods of interactive communications;
- to provide needed research data and training capabilities on issues that are experienced by every single countries from the region and our partners;
- to implement new curriculum and syllabuses aimed at compliance with the new military

doctrines and the accepted Partnership Goals;

- to improve the methods of research and training and the quality of our academic staff;
- to avoid simultaneous efforts on parallel projects and to increase considerably the effectiveness of resource spending;
- to provide immediate access to good practices and solutions related to interoperability;
- to improved the level of comprehension of studies and training;
- to increase the number of institutions and people that can benefit from the joint efforts;
- to use more effectively the resources provided through the Consortium, PIMS and NATO' TEEP Program;
- to increase significantly the return on investments made in our people and institutions by our partners.

In the long term, we can expect SEEDEFCOL to contribute:

- to strengthen existing and future centres of excellence;
- to raise the level of standardisation in military education;
- to increase the overall level of technology of military education and research institutions;
- to contribute to transparency of security initiatives;
- to contribute to the development of our own expertise in different forms of ADL and enlargement of the regional contribution to NATO and global efforts in research and training.
- to contribute to the changing of the military culture and gradual incorporation of democratic practices and culture of strategic thinking and acting.

Funding

Initial funding and financial support for SEEDEFCOL could be provided by the Consortium of Defence Academies and Security Studies Institutes. After discussion at a SEDM meeting, the funding issue could be raised at Working Table No. 3 of the Stability Pact. The issue could be addressed also to NATO TEEP Programme.

Initial material support could be provided through PIMS programmes.

Example of Immediate Input

Bulgaria can substantially contribute to the development of the curriculum of the SEEDEFCOL with its rapidly growing expertise in the fields of defence resources management, civil-military relations, including transparency of defence budgeting and regional security studies.

Nowadays, "G.S. Rakovski" Defence and Staff College is the leading national institution for higher education and qualification of military officers and civilian defence and security experts, as well as for scientific research on security and defence related issues, including interoperability with NATO.

The major tasks of the College are:

- to educate officers from battalion staff of all three services through a Master of Art programme in five specialties: Command and Control of tactical units of the Army, Air Force and Navy, and also Logistics and CIS, giving them a qualification for assignments as battalion commanders and staff officers in brigade and corps HQs;
- to educate and train senior military and civilian officers from the Ministry of Defence and the armed forces on national security, defence policy and planning, military strategy and campaign and operational planning;
- to organise and conduct a variety of post-graduate courses in specialised English and French Languages, training in NATO staff procedures, tactics and techniques and training for international assignments;
- to conduct scientific and applied research in defence related areas and to facilitate the achievement of technical interoperability;
- to provide a forum for open internal and international discussions on national security, defence policy, civil-military relations and democratic control over the armed forces.

New Academic Units

To fulfil its new tasks, new organisations were created in the "Rakovski" Defence College, supported adequately by infrastructure developments. For the purposes of SEEDEFCOL applicable are those units having the status of *centres of excellence*:

- The former General Staff Faculty was transformed into a *National Security and Defence Faculty*. The Faculty is carrying out senior level courses for civilians and military on *National Security and Defence Policy*.

  To support the curriculum a *National Security Information Centre* is producing electronic and printed materials and manages database with facts and analytical material about related issues.

  A newly establish *Centre for Civil-Military Relations Studies* was designed as Centre of excellence on the issues not only for the defence institution but also for the society.

- The *Interoperability Faculty* is tasked to transfer NATO and member countries' "know-how" in interoperability. This unit is the main tool for achieving the accepted Partnership Goals through education and training.

In the faculty an *English Language Testing Group* is established to develop and implement tests for evaluation the skills in accordance with STANAG 6001 (more than 1300 people were tested until the spring of 2001, about 900 of them passed the tests successfully). This group is recognized as a Centre of excellence in language testing and certification.

A College' *CAX Training Centre* is in process of creation. It will be fully equipped for training through simulations for PSO purposes and also to be used as remote site for international NATO-led and PfP CAX.

- The *Defence Advanced Research Institute* is designed to provide scientific support to defence reform and integration policy, to contribute for enhancing interoperability in doctrines and technology and for applying outsourcing and "off-the-shelf" opportunities in science and technology research.

  In the Institute an *international unit* is created and recognized as a *Centre of excellence in defence resource studies for the Pact of Stability for CEE*. In this capacity, the mission of the Centre is to contribute to the transparency in defence planning and to produce and share good practices for effective resource allocation.

  The Institute also includes a *Research and Demonstration Centre* for IT systems and equipment that could be of use for the purposes of the SEEDEFCOL.

The Way Ahead

In the next few years we expect revolutionary changes in security and defence related studies and military education and training. Distance learning, together with modelling and simulations, will change the way armed forces are trained. Increasing global competition, rapid technological advances, demographic changes, and the emergence of a service and knowledge-based economy impel military organisations to train and re-train their force in a new paradigm. Only these academies and colleges that deploy and effectively utilize ADL will have a distinct competitive advantage.

SEEDEFCOL could be the fastest way for the countries in SEE to explore this new frontier and to adopt web-based research and learning on a broad scale. The College could be the driver in the research and training in the coming years.

The first step was made during the Consortium' Annual Conference in Moscow, 2001 with the introduction of the idea by *Dr. Velizar Shalamanov*, Deputy Minister of Defence of the Republic of Bulgaria. That presentation is available on the Consortium's website.

The next step is planned during the IT Working Group meeting in Sofia, suggested for 10-12 December 2001. The Bulgarian Ministry of Defence invites all academic and research institutions from South East Europe and other EAPC defence education institutions, interested to cooperate, to

join the meeting.

Point of Contact:

Colonel Valeri Ratchev
Dean, National Security and Defence Faculty
"G. S. Rakovski" Defence and Staff College
E-mail: ratchev@md.government.bg

Notes:

1. SEDM – Southeast European Defence Ministerial.
2. EAPC – Euro-Atlantic Partnership Council.
3. ADL – Advanced Distance Learning.

BACK TO TOP

Author: **Information & Security**
Title: **Center for National Security and Defense Research**
Year of issuance: **2001**
Issue: **Information & Security. Volume 6, 2001, pages 167-169**
Hard copy: **ISSN 1311-1493**

CENTER FOR NATIONAL SECURITY AND DEFENSE RESEARCH

BULGARIAN ACADEMY OF SCIENCES

Table Of Contents:

The Bulgarian Academy of Sciences (BAS) is the largest national research center of Bulgaria, incorporating 76 research institutes and laboratories. It is one of the leading national institutions in the field of fundamental and applied research and technology development, including for research and development for the needs of the country's security and defense.

Taking into account the exceptionally important role of national security and recognizing the importance of the preparation for NATO membership as one of the main national priorities, the Bulgarian Academy of Sciences looks for effective mechanisms to carry out national security and defense research and to support the implementation of the National action plan for NATO membership.

The Framework Agreement between the Ministry of Defense (MoD) and the Bulgarian Academy of Sciences signed in December 1999 proved to be an important driver for activating and intensifying interdepartmental collaboration in the field of research and technology applicable to Bulgarian national security and defense. As a result of this agreement, in 2000 for the first time in ten years, scientists and experts from the Bulgarian Academy of Sciences joined en mass various projects and scientific events (workshops, symposia) in the field of defense and dual-use research and technology.

Bulgarian Academy of Sciences, being a national research institution that concentrates the basic research potential of Bulgaria, took up the task of scientific support for formulation and implementation of national security and defense policy and planning. With this purpose, the Executive Board (EB) of BAS established the "Center for National Security and Defense Research" (CNSDR) as an organizational coordinating unit to the EB of BAS.

Objectives and tasks

The principal objective of the CNSDR is to provide the necessary information, coordination and support to the BAS' units and individual scientists who take part in research activities in the area of national security and defense, in order to enable them to get deeply involved in the applied tasks faced by Bulgarian armed forces, Ministry of Defense and the Ministry of Interior in the processes of modernization and rearmament.

Principal tasks:

- To provide duly and accurately the necessary and definite information from the users in different branches of armed forces and administrative units of MoD to scientific and research teams of BAS.
- To provide information for the NATO Research and Technology Organization (RTO) and to commence working on the adaptation of suitable lines of research in the units of BAS involved.
- To support the establishment of goal-oriented teams and to coordinate their work on significant and important projects related to the modernization of the Bulgarian armed forces (BAF).
- To set up and coordinate bi-lateral cooperation and the cooperation with international organizations operating in the field of research and technology for national security and defense.
- To prepare and maintain a national database for the competence of research units, teams and scientists in corresponding scientific fields of priority for the national security and defense.
- To analyze and summarize in a bulletin national and international studies, the results of which may be used in the interest of security and defense.
- To organize and carry out national and international scientific events on the problems of research and technology in the interest of defense.

Organization and structure

The Center is established as a two-layer organization consisting of:

Management:

Supervising body is the Management Board of BAS, through its Council of National Security and Safety (CNSS), in concordance with the Interdepartmental Expert Coordinating Council (IECC) – joint council between BAS and MoD.

Staff:

The staff includes coordinators in corresponding branches of the national security and defense

research and the panels of RTO.

Executive units:

Research is conducted by program teams working on important and significant projects and consisting of scientists and engineers from various units of BAS where they have primary labor contact, but are functionally coordinated by the Center during the implementation of the project.

For contacts:

Center for National Security and Defense Research
Institute of Metal Science
67, Shipchenski prohod Str.
1574 Sofia, Bulgaria
Phone/Fax: +359 2 701053
E-mail: nsci@iusi.bas.bg

BACK TO TOP

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