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

Velizar SHALAMANOV

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.