C4I SYSTEM REENGINEERING:
ESSENTIAL COMPONENT OF BULGARIAN ARMED FORCES REFORM

Stoyan BALABANOV and Karmen ALEXANDROVA

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

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

The major objectives of this study were focused on achieving operational compatibility with the US and other NATO militaries. In order to achieve these objectives, conducted analyses and assessments of the current state of affairs and planned architectures in the field of C4I systems were taking into account the desired operational compatibility. Based on all that, the main recommendations and priorities for further development of C4I systems were defined.[2] In the course of the local

study, carried out in July 1999, a number of Bulgarian and US experts produced and exchanged preliminary reports through briefings. In the conclusive stages of the study the American experts submitted an official Final report.[8]

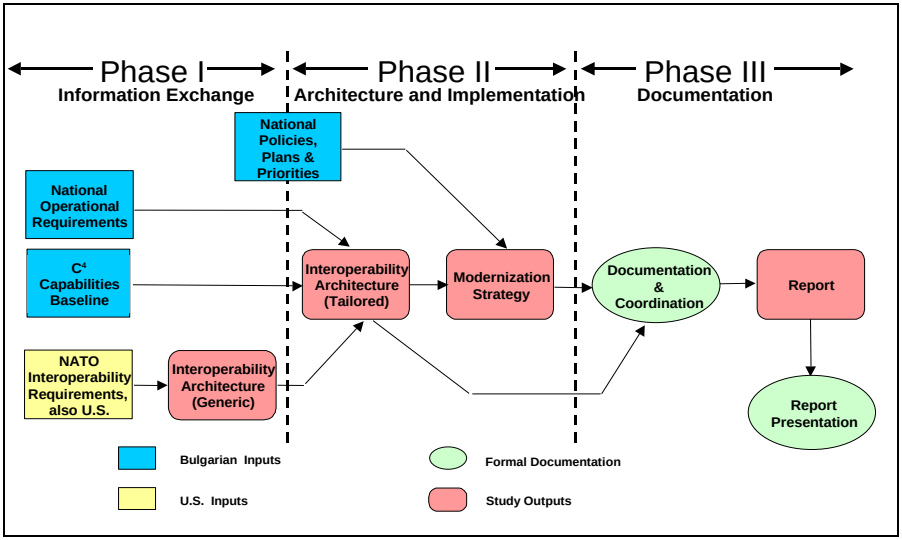

Figure 1. Functional Flow of C4I Study Process

This study proposed concrete and important steps towards improving:

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

We can point out as major achievements the adopted:

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

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

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

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

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

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

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

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

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

Achieving operational, system and technical compatibility

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

- Develop unified peacetime/wartime information systems;
- Programming project implementation;
- Wide use of COTS technologies

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

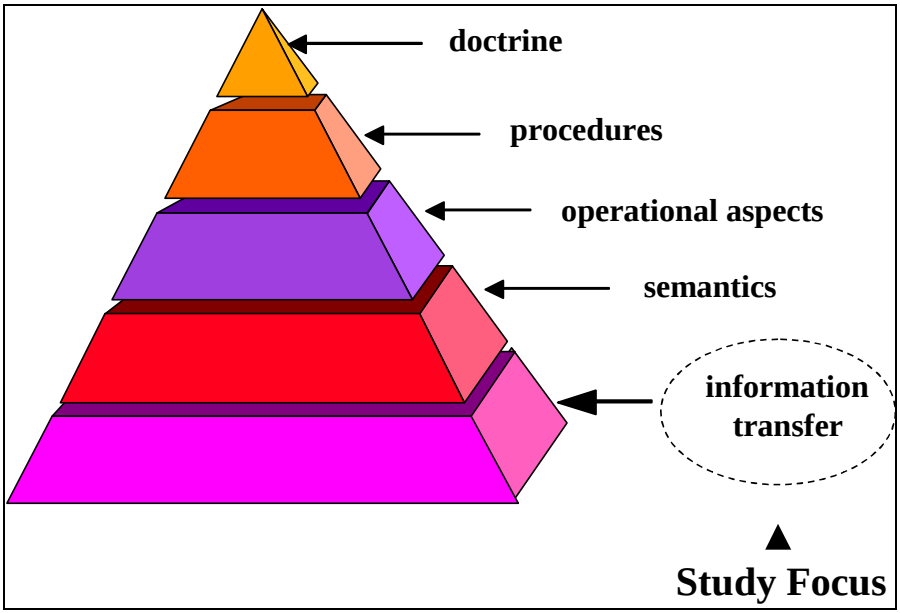

Figure 2. The Interoperability Pyramid

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

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

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

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

- Tactical area network interconnections established in accordance with EUROCOM D/1 interface specifications for voice systems. IP router-based interfaces using Guard technology to support e-mail exchange, with migration to ISDN connections in the future are also proposed;
- Single channel radio system interoperability for all Bulgarian military services compatible with NATO single channel radio STANAGs;
- Common Combat Net Radios (CNRs) for Bulgarian forces participating in multinational operations;
- Identification Friend or Foe/Selective Identification Feature (IFF/SIF) interoperability by implementing NATO-compatible interrogator sets and transponders and also Mode S Transponders compatible with ICAO, Annex 10;
- Finally, a comprehensive system security infrastructure that is fundamental to the interoperability architecture.

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

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

- Voice and fax service (clear and secure) provided by interconnection between the planned Bulgarian digital switched network and the Public Switched Telephone Network (PSTN);
- Secure message service provided by an extension of U.S. Defense Messaging System (DMS) (X.400 and SMTP gateways) through a leased digital connection to Bulgarian X.400 and SMTP gateways;
- Air operations communication support provided by U.S. tactical digital information data link extensions to Bulgarian entities and by exchange of formatted messages;

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

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

Recommendations for modernizing C4I systems and priority projects

The study addressed several additional C4 topics, among them Automated Management System Integration, Air Defense Modernization, Field Integrated Communication and Information System (FICIS), South East Europe Brigade (SEEBRIG) communications and information services, Data Networks, Network and Systems Management, Computer-Assisted Exercise, Collaborative Technologies, Information Technology and Management, System Acquisition and Information Assurance. These topics are vital, although not directly related to interoperability between Bulgarian and NATO/U.S. C4 systems. For these topics, the recommended

actions are independent from future NATO accession dates and, in some cases, are separated into short-term actions (up to 2 years) and long term actions (more than 2 years). The implementation prioritization of these recommendations is as follows:

CS AMS Integration

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

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

FICIS

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

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

SEEBRIG

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

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

baseline will be enhanced with C2. While developing this plan, the BAF should consider INFOSEC implications ahead of time.

Data Networks

The following actions should be accomplished in the short term:

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

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

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

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

Network and Systems Management (NSM)

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

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

CAX

The following should be accomplished in the short-term:

- Keep participating in Cooperative Automation seminar.

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

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

Information Technology and Management

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

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

System Acquisition

The following should be accomplished:

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

Information Assurance (IA)

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

- Update security policies to cover the entire scope of IA;
- Review and update existing security organizational responsibilities;
- Establish new organizational entities as required;

- Establish an incident reporting and monitoring capability;
- Establish system high LANs and WANs;
- Develop and maintain comprehensive security architecture;
- Begin introduction of 'protect, detect and react' capabilities;
- Implement firewalls;
- Implement Intrusion Detection Systems (IDS) on critical LANs;
- Establish network scanning and vulnerability assessment;
- Develop an IA training and indoctrination program.

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

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

Recommendations for the organizational structures related to systems development

Organizations

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

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

Defense Planning Directorate (DPD)

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

responsibilities in regard to C4I system development and maintenance in the Bulgarian armed forces.

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

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

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

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

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

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

"Information Support" Section in MoD

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

Information Support Center (ISC) - GS

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

Program/Project Teams

For the realization and management of projects carried out by external contractors it is advisable to designate programming teams, managed by the Chief Information

Officer and affiliated to IADR, Executive Agency "Central Military Support", or ISC – GH depending on the specific circumstances.

Other institutions

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

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

Chief Information Officer

Major institution in the MoD that coordinates and oversees the activities related to the management of the life cycle of C4I systems, as well as the coordination among various C4I system development programs, is the Chief Information Officer (CIO).

The responsibilities of the CIO are as follows:

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

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

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

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

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

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

- managing and using informational resources;

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

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

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

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

MoD Programming Council

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

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

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

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

The STC on C4I are established in:

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

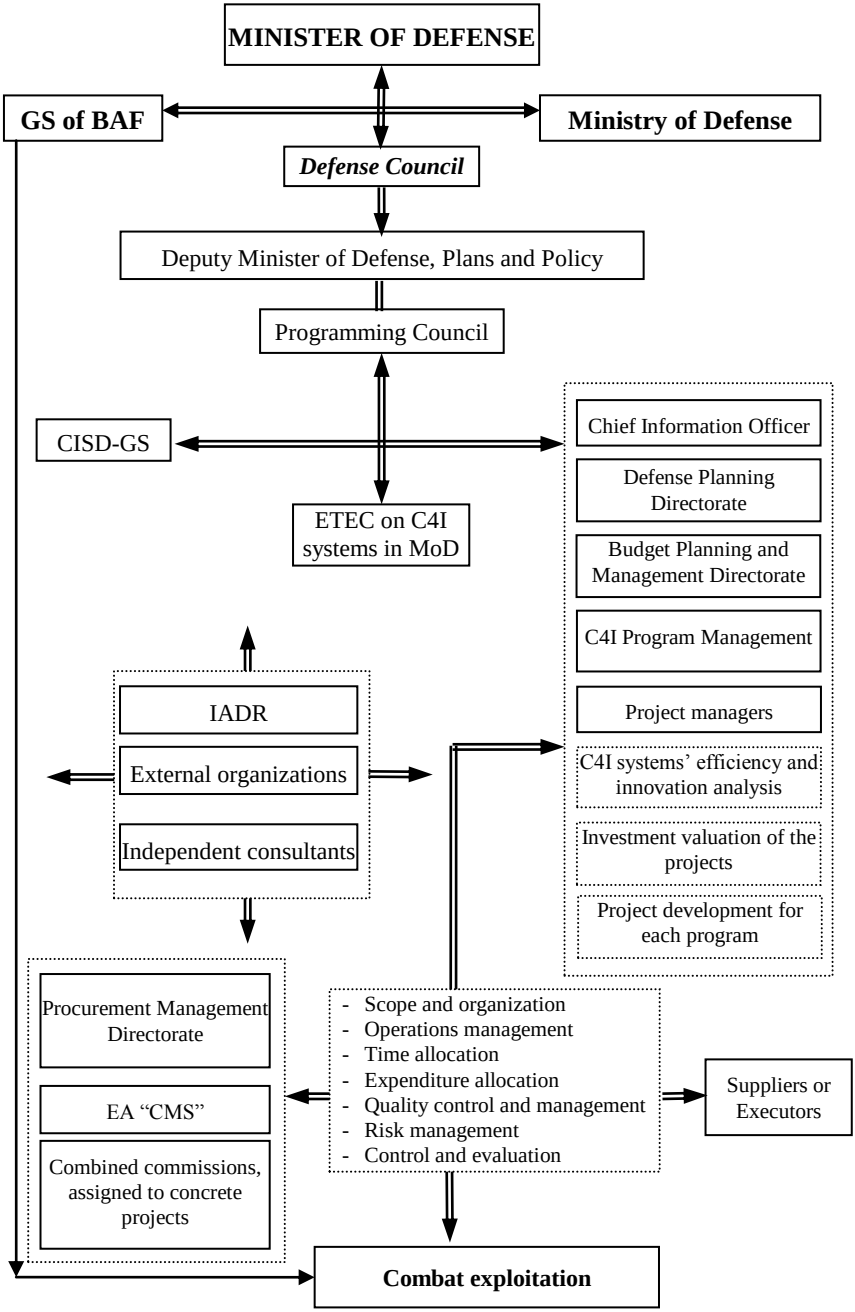

Figure 3. C4I systems life cycle management

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

Life cycle model of C4I systems

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

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

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

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

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

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

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

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

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

(9) The scientific supervision in the course of the projects' experimental-design stages is done by the IADR. The Procurement Management Directorate carries out

activities related to commercial contracts. The EA "CMS", the Military Standardization, Certification, and Codification Directorate (MSCCD) and the Security Service in MoD are responsible for organizing the testing, correctness of standardizing documents, certifying the producers and information control and protection in C4I systems.

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

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

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

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

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

Conclusions

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

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

After proving its indispensability, the institution of the Chief Information Officer was established in the MoD of the Republic of Bulgaria. The Chief Information Officer is responsible for development of C4I systems in MoD, coordination and management

of the undertaken projects aiming at the effective use of new information and management technologies.

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

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

References:

1. *Military Doctrine of the Republic of Bulgaria*, Approved by the XXXVIII National Assembly of the Republic of Bulgaria on April 8, 1999, (Sofia: Military Publishing House, 1999). Full text in English is available at http://www.md.government.bg.
2. *Main Recommendations for Development of C4I Systems in the Bulgarian Armed Forces* (Sofia: Ministry of Defense, 2000).

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

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

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