BULGARIAN INFORMATION NETWORK: COMMAND INFORMATION INFRASTRUCTURE FOR THE FUTURE

Daniel F. WIENER II and John COURTIEN

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.

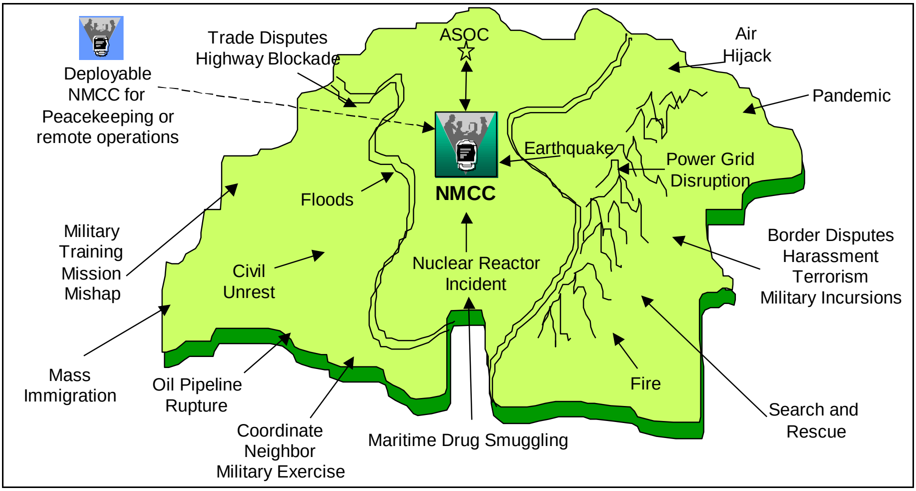

Figure 1: NMCC Support to Crisis Management Operations

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 2. [2]

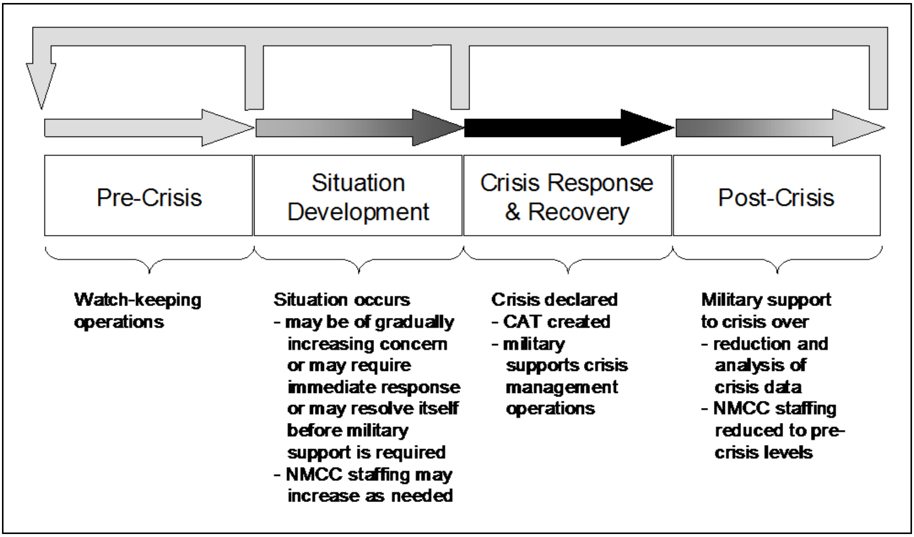
Pre-Crisis
Situation Development
Crisis Response & Recovery
Post-Crisis
Watch-keeping operations
Situation occurs
- may be of gradually increasing concern or may require immediate response or may resolve itself before military support is required
- NMCC staffing may increase as needed
Crisis declared
- CAT created
- military supports crisis management operations
Military support to crisis over
- reduction and analysis of crisis data
- NMCC staffing reduced to pre-crisis levels

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.

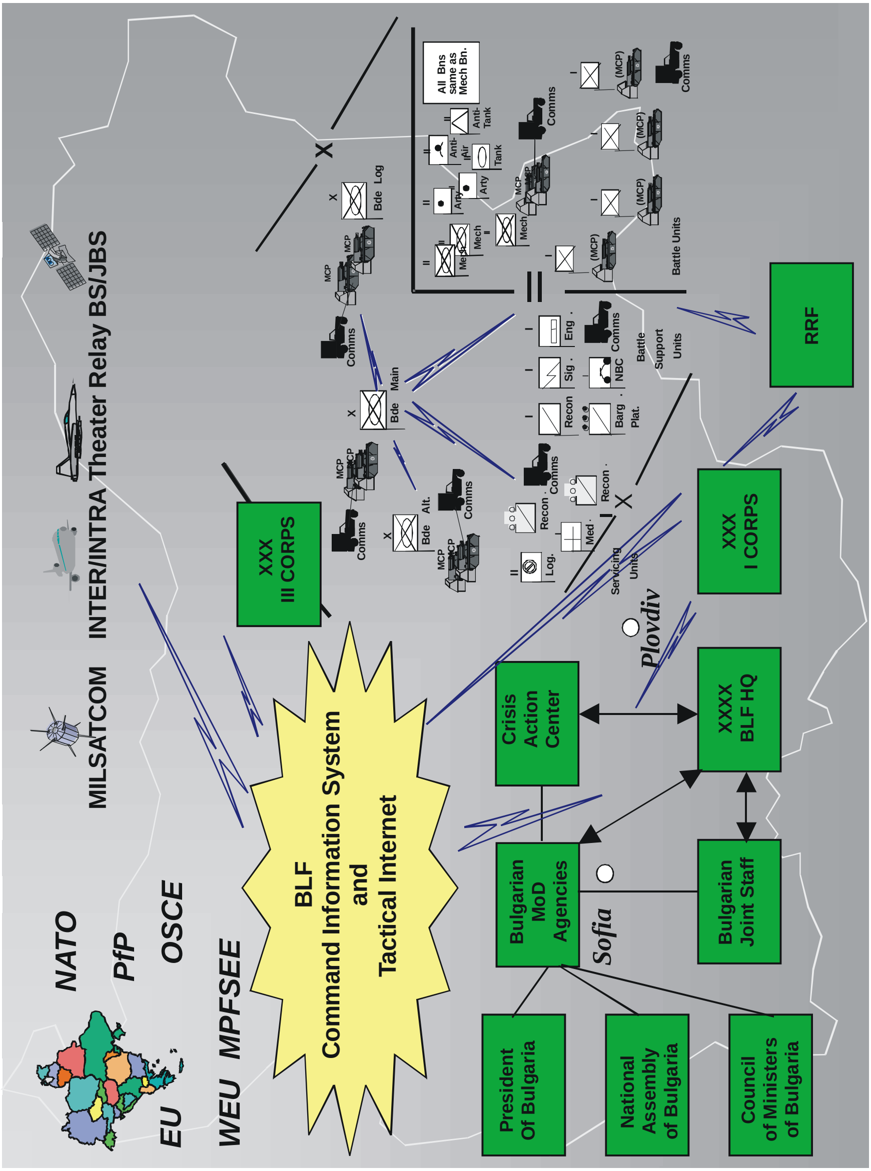

Figure 3: High-level Operational Graphic

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.

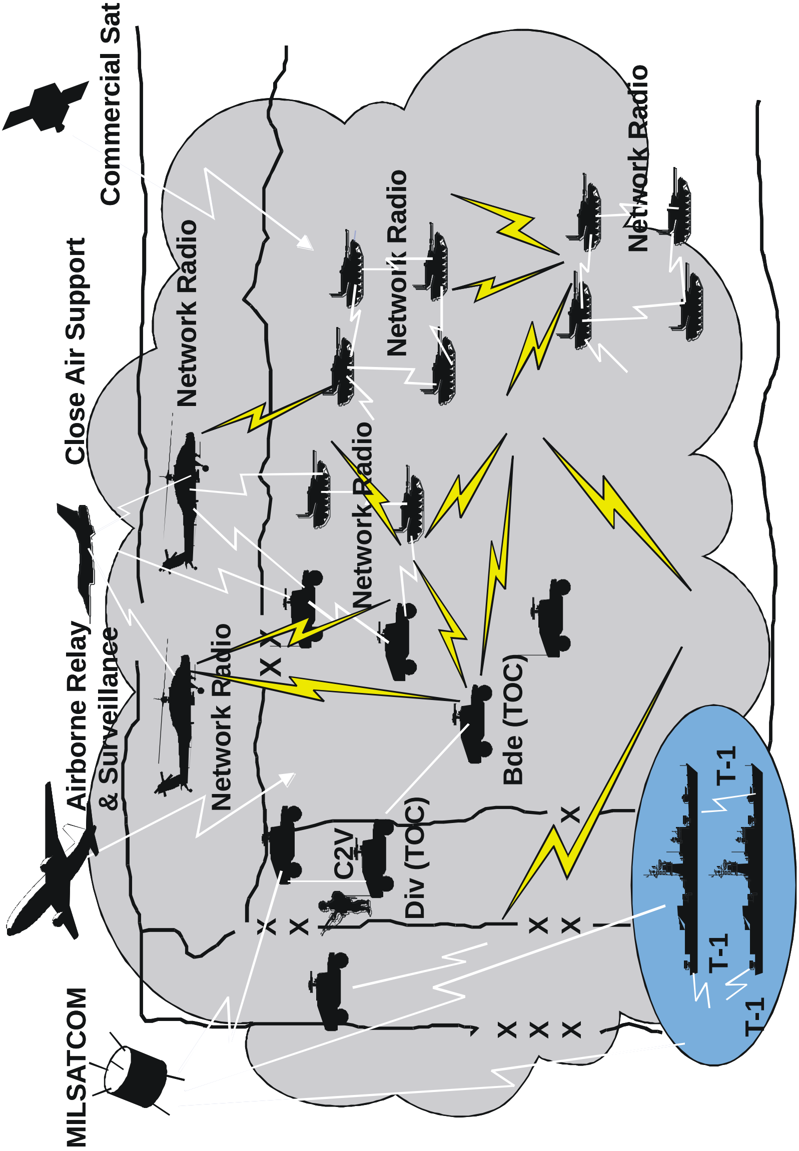

Figure 4: A notional implementation

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