"Mircea cel Batran" Naval Academy Scientific Bulletin, Volume XIX – 2016 – Issue 1
Published by "Mircea cel Batran" Naval Academy Press, Constanta, Romania // The journal is indexed in: PROQUEST / DOAJ / DRJI / JOURNAL INDEX / I2OR / SCIENCE LIBRARY INDEX / Google Scholar / Crossref / Academic Keys / ROAD Open Access / OAJI / Academic Resources / Scientific Indexing Services / SCIPIO

INTERCONNECTING NETWORKS WITH DIFFERENT LEVELS OF SECURITY – A PRESENT NATO PROBLEM

Liviu TATOMIR[1]
Bebe IONASCU[2]
Stefan POPA[3]
Alexandru BARBU[4]
Ciprian DRAGOI[5]
[1]Scientific researcher II, Eng. Military Equipment and Technologies Research Agency, Bucharest
[2]Scientific researcher III, Cpt. Eng. Military Equipment and Technologies Research Agency, Bucharest
[3]Scientific researcher, Cpt. Eng. Military Equipment and Technologies Research Agency, Bucharest
[4]Assistant Researcher, Cpt. Eng. Military Equipment and Technologies Research Agency, Bucharest
16 Aeroportului street, Clinceni
[5]Assistant Researcher, Slt. Eng.Military Equipment and Technologies Research Agency, Bucharest

Abstract: *A situation often met in the Romanian Armed Forces in recent years is the need for interconnecting two networks (domains) with different levels of classification. Considering that the Romanian armed troops are involved in numerous missions with NATO partners, solutions, already implemented across the organization, are considered to be applied in domestic systems, also. This paper presents the solutions adopted by NATO in order to solve the problem of cross-domains interconnections. We present the maturity level reached by these solutions and the possibility of implementing these solutions in the Romanian Armed Forces, with or without specific adaptation to our own rules and regulations. The goal is to use a NATO already proved solution to our national classified networks.*

Keywords*: Informatics, Networks, Interconnection, Communications*

Introduction

A problem currently faced by the Romanian army is exchanging information between networks with different classification levels. The following are examples of situations encountered in some of the Romanian Army' Land and Naval forces. The cases presented were encountered during missions carried out in the respective units:

- Interconnecting fighting vehicle platforms at group / platoon / company level with their battalion command post. In this case it is necessary to send orders and informations about the tactical situation in a high-low manner (from the battalion command post to the fighting vehicle platforms) and also require the submission of reports, applications and specifical tactical informations in a low-high manner (from the fighting vehicle platforms to the battalion command post). Considering that at the battalion command post level there are 2 classified networks - one "unclassified" and the second "secret" and the classification level of the informations at the platforms level cannot exceed "restricted" for security reasons, a question arises: how can we achieve information exchange between the "secret" network at the battalion command post level and the platforms that can only use "restricted" classified informations?
- Interconnecting a comandament ship with the subordinated ships in order to integrate the sensors from the subordinated ships in the comandament ships' command-control system. This case is very similar to the above one, meaning that the classification level of the subordinated ships' communications and information system cannot exceed the "restricted" level and the comandament ships' communications and information system cannot be classified under the "confidential" level, because it comprises the command-control application.

The same problem occurs in both of the situations described above: how can we exchange information between 2 or more networks that have different classification levels?

Because national and NATO regulations on how to interconnect networks with different levels of classification are quite elusive in terms of the proposed technical solutions (as it will be explained below), the examples presented above are yet to be solved by the national military structures responsible in these tasks.

The examples presented clearly show the need to transfer informations between networks with different classification levels, but at the same time it is obvious that there is a need to keep a balance between the newly acquired functionalities and the security risks involved by these capabilities.The security risks involved are determined by the following factors:

- Leaking information from networks with higher classification level to networks with lower

DOI: 10.21279/1454-864X-16-I1-087

classification level, information that has a higher classification level than the destination network.
- Cyber attack on networks that are circulating classified information in order to damage the hardware and / or software of these networks, or to extract classified information.

Also, another important factor that needs to be taken into account when seeking interconnection of several networks with different classification levels is that the networks can have different technical, procedural and security characteristics (as it happens in most cases). NATO has tried to standardize these situations, as it will be shown below, but the development of all aspects involved in this case is far from being completed.

The NATO regulatory framework regarding CIS interconnection

Currently, in NATO, the implementation of communications and information systems (CIS), as the definition of the interoperability level between them is governed by the following documents:

"NATO Information Management Policy" – a NATO document that establishes the way in which the management and security of information are made in the organization.

"Allied Joint Doctrine for Communication and Information Systems" (AJP-6) – represents the integration doctrine of CIS systems in the joint NATO operations. It describes the characteristics and the structure of CIS systems and also the roles, responsibilities and the command and control process in the CIS systems. Regarding the interoperability, the rules for achieving interoperability are set for the land, sea and air structures, as well as the documents governing the interoperability of the these structures:

- for land forces: STANAG 5048 and "Multilateral Interoperability Programme" (MIP);
- for naval forces: MC 195/8 and ACP-200B;
- for air forces: the reference architecture for Air Command and Control System (ACCS);

"Primary Directive on CIS Security" – establishes the security requirements that a CIS system must meet in order to ensure a certain level of data protection.

"Security Within the North Atlantic Treaty Organisation" – establishes the security measures needed for the protection of CIS systems, measures aimed at ensuring the confidentiality, integrity, availability, authenticity and non-repudiation of the information transmitted within these systems.

"INFOSEC Technical and Implementation Guidelines for Cisse Interconnection" – the most important document in terms of interconnecting classified CIS systems. It establishes the requirements for interconnection of communications and information systems that process NATO classified information, as follows: between a NATO CIS and a non-NATO CIS, between a NATO CIS and another NATO CIS and between a NATO CIS and Internet / similar networks in the public domain.

As can be seen, in terms of the procedural and technical way, the interconnection of two networks is well covered by the existing NATO standards. However, when it comes to the interconnection of two networks with different classification levels, this is not explicitly defined in any document.

But there are attempts with regard to this issue, both theoretically and from a practical standpoint. In NATO, to date, there are only two solutions allowing the interconnection of two networks with different classification levels. These concepts are described below, a major emphasis being given on the maturity level reached by each of these solution.

IEG (Information Exchange Gateway)

IEG's (Information Exchange Gateway) is a concept introduced by NATO in order to facilitate secure communication between systems with different security and management policies, by providing a set of services with the following functionality: protection of network infrastructure against external threats, implementation of security policies on traffic transiting the IEG, the sharing of information between networks using proxy servers.

Implementation scenarios for IEG's were defined by NATO on the following parameters:

- the classification of networks that is intended to be connected;
- the classification level of information circulating between networks;
- authorities that operate those networks;
- security policies implemented at the level of those networks;
- NATO interconnection with other various systems (international organizations / NGOs / INTERNET / unclassified systems);

Considering the aspects that were just presented, NATO has developed five possible scenarios for the interconnection of networks with different classification levels through IEG's, scenarios shown in the following figure:

DOI: 10.21279/1454-864X-16-I1-087

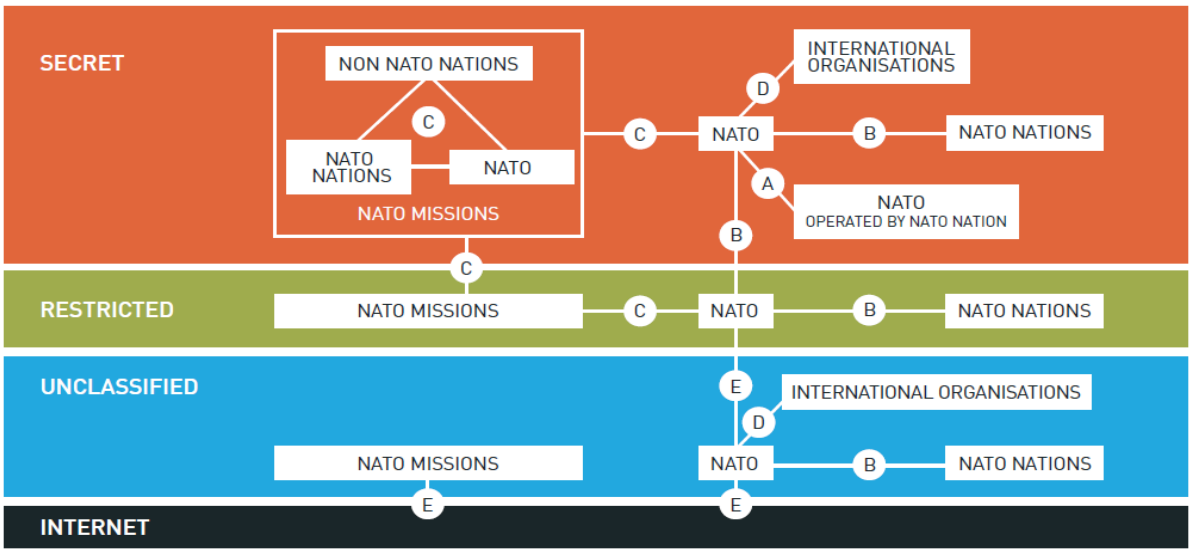

Figura 1. The five scenarios of interconnection through IEGs (A, B, C, D, E)
of networks with different classification levels

The 5 scenarios are defined as:
- Scenario A is defined for connecting two domains that have the same security classification level and same NATO baseline CIS, but are operated by different authorities. Typically, this will be a NATO enclave run inside a NATO nation.
- Scenario B is defined for connecting two domains that have the same security classification level, but different security policies, for example a NATO nation connecting to NATO. Scenario B variants also cover connecting multiple/different security classification levels with the same security policy, for example NATO Secret to NATO Restricted.
- Scenario C is defined for connecting deployed NATO mission systems to other domains.
- Scenario D is defined for connecting NATO systems to international organisations or non-government organisations.
- Scenario E - is defined for connecting NATO systems to the Internet or NATO systems to NATO Unclassified systems that are connected to the Internet.

As already presented, an IEG enables the exchange of core network information and also mission information (functional services) by providing protect functionality to the network infrastructure against external threats and by implementing security policies to the traffic transiting the IEG.

It can be seen that although the theoretical and procedural component of the IEG is well established, the technical implementation of IEG's is left at the enterprise’s discretion, any equipment not being standardized for this purpose.

A functional block diagram of an IEG is shown in the following figure:

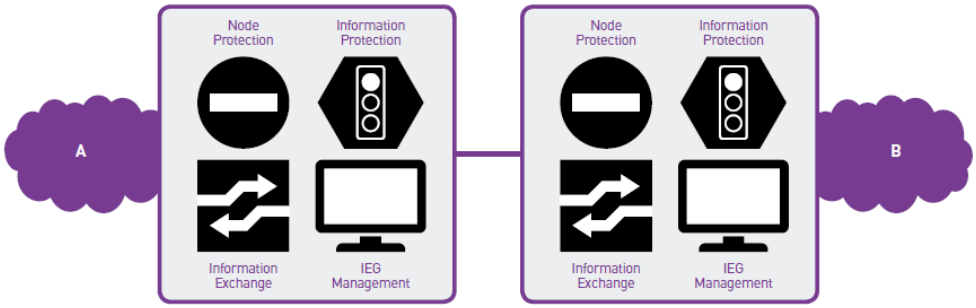

Figure 2. The block diagram interconnection through two IEG's (the picture is taken from the paper "Information Exchange Gateways: Reference Architecture" Nexor, 2009)

DOI: 10.21279/1454-864X-16-I1-087

It can be noted that an IEG is structured as an interface with the standard functionalities described above. From the previous figure we can deduct the functionalities met by an IEG:

- Node protection - protects the hardware and software infrastructure through services such as filtering, intrusion detection and virus detection;
- Information Protection - protects the domain data by implementing security policies such as checking the information when exiting the domain;
- Information exchange - is controlled through the use of proxy servers that allow only certain types of information to be exchanged;
- IEG management - conducted to verify the correct operation of IEG.

The following is a technical implementation of a IEG solution made and tested by the British company Nexor:

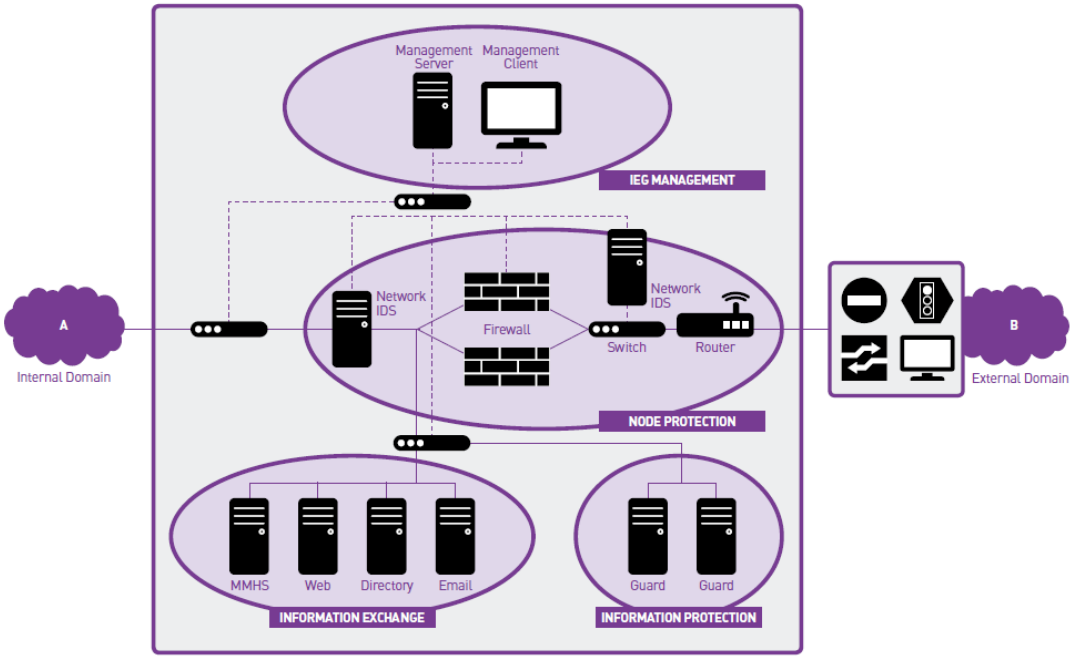

Figure 3. The technical interconnection between two systems using IEG's (the picture is taken from the paper "Information Exchange Gateways: Reference Architecture" Nexor, 2009)

Another technical solution for implementing an IEG is made public by the British firm Deep Secure. In the "Implementing Deep-Secure guards in NATO Information Exchange Gateways" paper, paper made public by Deep Secure in 2014, technical solutions specific to this company are described, technical solutions that implement the functionalities of an IEG (services such as exchanging web traffic, email, formal messaging, files, chat, SNMP, XML etc. being supported). In the following figure, the correlation between the usage scenarios of an IEG, the services provided by an IEG and the Deep Secure products that perform these services is presented (the picture is taken from the paper "Implementing Deep-Secure guards in NATO Information Exchange Gateways" Deep Secure, 2014):

IEG Scenario	Deep-Secure Products	Information Exchange Services
A	None	N/A
B (1) Protecting NATO	None	N/A
B (1) Protecting Nation	• Web Guard; • Mail Guard; • FTP Guard; • TransGap; • Chat Guard.	• Web Browsing; • Web Services; • Email; • Formal Messaging; • File Exchange; • Directory Replication; • Chat.
B (2)	• XML Guard; • Minerva; • NetMan Guard.	• Any HTTP based XML transfer; • SNMP / Syslog.
C	• Web Guard; • Mail Guard; • FTP Guard; • TransGap; • Chat Guard.	• Web Browsing; • Web Services; • Email; • Formal Messaging; • File Exchange; • Directory Replication; • Chat.

Figure 4. The technical implementation of an IEG made by the Deep Secure company

DOI: 10.21279/1454-864X-16-I1-087

During 2015, the British company Deep Secure, alongside NATO's NCI and a structure of the Italian Air Forces (Re.GISCC – Command and Control Systems and Innovation Management) managed to complete an IEG for the Italian Ministry of Defence, IEG accredited at both national and NATO level according to Common Criteria. This IEG enables information sharing between the Italian Ministry of Defence and NATO and other coalition partners. The information that can be exchanged are core information, like mail, web and network management services, and also mission-specific information (functional services such as chat, Link1, Link 11B and Link 16).

During 2016, the Nexor company has presented in its paper "Connecting multiple networks securely" the way they are involved, along with Lockheed Martin, in providing a secure network infrastructure solution for a major European program. The paper states that the network infrastructure solution must be able to exchange information with other domains, for this purpose the network infrastructure has an IEG based solution certified by Nexor: Nexor Sentinel (email gateway accredited under the Common Criteria at EAL 4+ level), Nexor data diodes (data diode built in gateways, evaluated according to Common Criteria EAL 7+ level), Nexor Guardian and Nexor Border Gateway.

It can be concluded that there are commercial eneterprises that can produce both components for IEGs, components that are accredited by third-parties and also complete solutions for IEGs, solutions that are customized to the users' needs.

From the examples presented so far, it can be concluded that there are companies that can deliver complete solutions customized to the users' requirements, and also companies able to provide accredited hardware and software equipments that fulfill specific IEGs functionalities. However, it can be said that the IEG as a concept is still in the development/ understanding phase, given the fact that there are still many questions arising, especially from those who are considered beneficiaries of this product in terms of its functionality and technical implementation.

Regarding the possibility of implementing this solution in the Romanian Army in order to solve the problems described at the beginning of this paper, there are no major procedural or technical issues regarding the implementation and the use of IEGs in the Romanian Army. However, there are certain issues that could prevent the introduction of IEGs in the Romanian Army, issues whose importance can only be established by Army authorities at a high decisional level:

- the very high level of technical training involved in using and ensuring the maintenance of the solution. It requires very high knowledge in areas such as computer, networking and communications, areas with a low number of specialists in the Romanian Army.
- because the hardware and software implementation of this solution requires a high space volume and also an increased level of energy consumption, it is possible that the IEGs do not represent a feasible solution for the vehicular, air and sea platforms, where these resources (space and energy) are limited.
- the high cost of these solutions. Although we do not have an estimated cost for IEGs, mainly because these solutions are customized for each beneficiary based on its requirements, it's obviously that adopting this solution will require high costs. That means that the adoption of this solution on a wider level (eg. in the Romanian Army) can be prohibitive.

Data Diode

An equipment that has an important role in the interconnection of networks with different levels of classification is the data diode. This equipment can be used both as stand-alone equipment and also as part of an IEG, allowing the transfer of information in a single direction. Using this equipment greatly increases the level of confidentiality of the conveyed information, but also it affects the integrity and the availability of the data being transferred.

As certain communication protocols requires a session between the correspondent two sides to be performed, it means that using a data diode would completely brake the communications based on such protocols. In this regard, to avoid these situations, in the composition of a data diode usually we find two proxy servers, one on each side of the diode data. These servers are designed to extract the meaningful information from the data packets, useful information that is then passed to the other side of the diode where the matching proxy server reintroduce the useful information back into the data packets. In this way, the attacks hidden in the data transport protocol are neutralized.

The use of data diodes is recommended in two cases: for information protection (as can be seen in the upper part of Figure 5, the higher classification level network cannot transfer any data to the lower classification level network), and also for physical goods protection (as can be seen in the lower part of figure 5, the diode can be configured so that the lower classification level network cannot transmit some type of information to the higher classification level):

DOI: 10.21279/1454-864X-16-I1-087

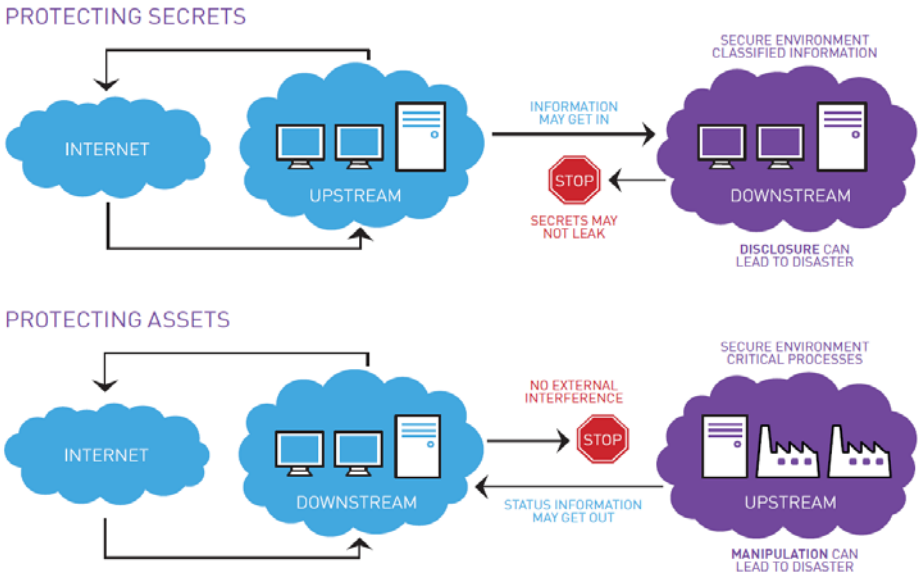

Figure 5. The way the information and physical goods are protected via diodes (images are taken from the paper "Protecting confidential information on Using diodes", Nexor, 2015)

Data diodes are already used to interconnect domains with different levels of classification, in cases where the security risks are very high. A quick Internet search reveals that there are numerous international companies producing such equipments, many of them certified according to Common Criteria level EAL7+ and that are already used in the operational environment (BAE Systems, Nexor).

It can be concluded that the maturity level achieved by these devices is quite high, certainly higher than the IEG's. But are these devices suitable for solving the existing problems in the Romanian Army, problems described in the introduction to this paper? The simple answer would be yes, and the justification is that the data diodes can be used to allow the transfer of the information only in a one directional way (from the lower classification level network to the higher classification level network), however, if desired, a bi-directional information exchange can be set up, through the implementation of two diodes (one in each direction), which will operate in parallel.

Also, in terms of complexity, even though these solutions are not easy to deploy, they are much simpler to understand and to use than the IEGs. In terms of costs, in the paper "Date Diodes for Cyber Security" (available at INTERNET complicated http://courtneybarry.com/Images/TS_Data_Diodes.pdf) such equipments are estimated between 30,000 and 150,000 U.S. dollars, depending on the ensured bandwidth, EAL level, mean time between failure and other parameters.

The FMN concept (Federated Mission Network)

The second solution that can be used to perform the interconnection of two (or more) networks with different classification levels is to implement the Federated Mission Network (FMN) concept. The FMN concept was developed based on the best practices and lessons learned by the allied troops from completing the missions in Afghanistan. The FMN concept is to establish a mission network federation capability, allowing the efficient exchange of information between the entities participating in military operations (NATO member countries and / or non-NATO). The FMN role is to provide a common framework for the organization of a mission (operational requirements, principles and considerations for implementing the mission network federation capability) and also to provide a complete framework for interconnecting participating forces.

The FMN capability has three major components: governance, FMN framework and mission network (MN), as illustrated in the following figure:

DOI: 10.21279/1454-864X-16-I1-087

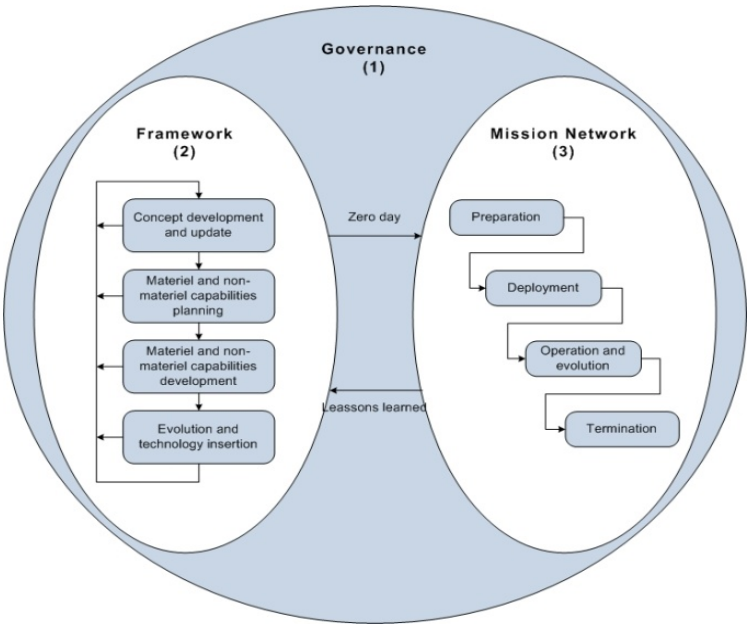

Figure 6. The components of the FMN capability

Governance provide the environment within which effective management of the other two components occur.

FMN Framework is the structure providing processes, plans, templates, enterprise architectures, capability components and tools needed to prepare (including planning), develop, deploy, operate and evolve and terminate Mission Networks in support of Alliance and multinational operations in dynamic, federated environments.

Each MN is a tailored capability created for the purpose of an operation, exercise, training event, and/or interoperability verification activity. MN includes non-material (policy, processes, procedures and standards) and material (communication and information systems - CIS) contributions provided by NATO, NATO Nations and Non-NATO Entities participating in operations. In this kind of federation each participant retains control of own capabilities while accepting and complying with the requirements laid out in pre-negotiated and agreed arrangements in a collective fashion.

The FMN concept defines four levels of capability that provides options for the participants in the mission network, particularly in terms of effort and commitment of resources for those affiliated to the FMN:

a. Option A - Mission Network Element (MNE). A MNE contains networking and information infrastructure and services for self-provisioning. At this level, a MN participant will be able to provide interconnection to Option B participants, and may provide mission essential services to specific Option B and Option C participants if appropriate agreements exist.

b. Option B - Mission Network Extension (MNX). A MNX contains infrastructure and services for self-provisioning, but may not include sufficient mission essential services. At this level a MN participant may be provided with mission essential services from an Option A participant.

c. Option C - Hosted User. A Hosted User is a MN participant that is not able to provide infrastructure and services for self-provisioning. This participant will typically be embedded in an MNE or an MNX.

d. Option Z - Other Entities. The other participants are not an integral part of the network, nor are they subject to FMN Framework requirements, but they enable the exchange of selected information products. Interconnection and information exchanges with these participants are made by Option A and Option B participants on a case-by-case basis. This kind of interconnection typically involves the use of information exchange gateways.

In the FMN concept, the main resource is the information. This means that each MN provides a common mission information domain that enables the efficient exchange of information. Also, in the FMN concept, the CIS security focuses on the protection of the information itself. This is a different approach from the traditional systems where the areas of security are protected. Thus, FMN proposes a new standard relating to the labeling of information in terms of confidentiality. In a multiple entities scenario, each governed by different security policies, information exchange is based on individual bilateral agreements. The objective of the new standard is to provide common implementation-independent

DOI: 10.21279/1454-864X-16-I1-087

formats and syntax for security policies and confidentiality metadata so that all information objects and data assets can be labelled to support access and release decisions in a manner that is understandable to all coalition partners.

This is the great novelty of FMN's: the concept of network-based information - the information can travel freely, based on the confidentiality label. The confidentiality label includes the following major elements: the governing security policy, classification, privacy mark, category.

Regarding the implementation of the FMN concept in the Romanian CIS systems, this implies the introduction of a mechanism for labeling and binding in accordance with NATO requirements. Thus, Romanian CIS systems must be upgraded to be able to share information with future FMN networks. Moreover, the level of capability that we want to choose in order to contribue to the network mission must be decided: MNE, MNX or host user. Any of the capabilities is chosen, the system architecture must be in line with the FMN architecture, as defined in the FMN Implementation Plan.

It can be seen the high degree of complexity regarding the introduction of the FMN concept in the Romanian Army. This is not considered at the moment, but if in the future it will be decided that we need to to achieve this goal, all the details involved by this change must be put to place by a large number of military structures, namely: operational, logistical, technical, research, and all the categories of forces (land, air, sea).

Regarding the degree of maturity reached by the FMN concept, it is still in the developing stage. NATO is continuing the effort to operationalize the FMN concept both nationally and at the NATO level, the main areas of interest being doctrine, how to join FMN, testing the concept, joining the NATO Defence Planning Process. The FMN concept has been tested during the CWIX exercises (Coalition Warrior Interoperability Exploration, experimentation, examination, exercise) in 2013, 2014 and 2015, and also will be tested in the CWIX exercise that will be held this year. Also, the FMN concept was tested during the Steadfast Cobalt and Trident Juncture exercises, in 2015.

In early 2015, NATO Federated Mission Networking Implementation Plan (NFIP) was approved by the North Atlantic Council (NAC), which led to the intensification of technologies, standards and configurations of communications and information networks transformation, in order to implement the FMN capability.

The market study conducted by NCIA this year

As a proof that the existent NATO solutions have not reached a high maturity level, so that the reliable interconnection between two networks with different classification levels can be easily achieved, is the market survey conducted this year by NCIA (NATO Communications and Information Agency) on the existence of commercial products that could be used as Boundary Protection Devices (Border Protection Equipment) - BPD. In this market study, all commercial companies resident in Member States of NATO that are producing equipments such as BPD are invited to contact NCIA to describe the capabilities of the products they produce.

In the market study are described, at the begining, the solutions expected by NCIA to ensure the interconnection between systems with different levels of classification (NATO SECRET - NATO UNCLASSIFIED and NATO SECRET - NATO NATO RESTRICTED). As expected, the solutions they expect are similar to those identified in this paper, namely:

- hardware data diodes with applications gateway;
- multilevel security system.

Characteristics to be met by the proposed solutions are:

- solutions must be certified Common Criteria EAL 4+ or a higher level for the protection profiles specified in the market research;
- solutions must be based on COTS products (Commercial Off The Shelf);
- solutions must meet the requirements of the following NATO documents: "Primary Directive on CIS Security" and " Management Directive on CIS Security";
- solutions must meet the NATO security requirements specified in the "INFOSEC Technical and Implementation Directive for CISs interconnection";
- NATO solutions must meet the security requirements for NATO SECRET systems specified in "INFOSEC Technical Implementation Directive for Computer and Local Area Network (LAN) Security";
- solutions must provide port-based and IP traffic filtering on its borders;
- solutions must be capable of processing real-time traffic.

CONCLUSIONS

As a conclusion regarding the technologies and concepts presented in response to the current issue in the Romanian Army – the need to interconnect two or more CIS systems with different levels of classification – the existing solutions found in NATO, even if they have not reached a very high maturity level, are in a continuous development and improvement process. The optimal solution identified is one that requires the

DOI: 10.21279/1454-864X-16-I1-087

use of data diodes for connecting CIS systems. These diodes are used in at a global level, not just in NATO, do not involve changes in CIS system architecture, have the lowest costs of the presented solutions and there is a large number of manufacturers of such equipments.

The IEG (which may also include data diodes) is a concept that was introduced and standardized by NATO and that has not reached the anticipated development level. Since it is a difficult concept to understand for the user, and, moreover , difficult to implement, IEG's are developed and implemented by the military in close collaboration with the manufacturers of such solutions, as there are not a lot of public information about IEGs. However, given the fact that the IEG addresses and provides the solution to the same problems addressed by the FMN concept (concept that seems to be a priority for NATO), its future seems uncertain.

The FMN is, as the IEG, a concept developed by NATO to improve communication between partners. But unlike it, FMN involves major changes in NATO nations' CIS systems, changes that will be certainly reflected in the implementation cost of this concept. Currently, the FMN is still in the testing phase in multinational exercises, but the support level from NATO makes us believe that it will not be long until all the Member States will start implementing this concept.

BIBLIOGRAPHY

[1] "NATO Information Management Policy " NATO
[2] "Allied Joint Doctrine for Communication and Information Systems" (AJP-6), NATO, aprilie 2011
[3] "NATO FMN Implementation Plan Version 4.0" NATO, 30 September 2014
[4] "Primary Directive on CIS Security" NATO, 15 noiembrie 2013
[5] "Security within the North Atlantic Treaty Organisation" NATO, 17 iunie 2002
[6] " INFOSEC Technical and Implementation Directive for CISs interconnection" NATO
[7] "Information Exchange Gateways: Reference Architecture", Nexor, 2009
[8] "Data Diodes for Cyber Security", Cooperative Research Network, martie 2012

DOI: 10.21279/1454-864X-16-I1-087