Federated Mission Networking (FMN) concept was developed in order to ensure global rules for establishing a federation of Communication and Information Systems (CIS) organized in a Mission Network (MN) to “enable effective sharing information among NATO, NATO Nations and/or Non-NATO entities participating in operations”, according to “NATO FMN Concept”. One of the major aspects of the management of information in such network is the security of shared information, in particular confidentiality. In the digital environment, confidentiality of shared information regardless of its format can be assured using confidentiality labels. The paper aims to outline how NATO requirements on labeling information can be implemented in Romanian CIS, both for legacy system as well as future systems in the way that they can achieve the FMN objectives in a national MN and/or coalition MN.

FMN Components

The FMN capability consists of three components: (1) Governance, (2) FMN Framework and (3) Mission Network (MN) as illustrated in the Figure 1. 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”. [1] 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.

There are other three notions used by FMN concept: Mission Thread, Day Zero and Common Information Domain. Mission Thread (MT) represents an operational and technical description of the end-to-end set of activities required to execute a mission or mission task, so it describes operational processes and information products. Common Information Domain represents an environment where there is open sharing of information underpinned by mutual trust and governed by a common rule set. The Entities participating in operations decide individually what information is shared within this common information domain. The domain may contain one or more security levels.

Day Zero is the moment when the requirement of a MN is identified. It is the start point of a tailored MN. MN Day Zero capability refers to the minimum capabilities required to support the needs of the Commander during the pre-deployment and initial deployment phases of an operation. But the NFIP ([2], [3]) considered that this notion is not adequate to express the capabilities required to ensure the rapid availability of a Mission Network, so it introduces four environments:

a. Verification and Validation (V&V) Environment used to evaluate the interoperability of capabilities before they are required for an exercise or mission, verify technical and procedural interoperability of proposed service solutions, including V&V of CIS Security for FMN Affiliates.

b. Collective Training Environment enables the collective preparation, staff training, exercising, and mission rehearsal of the headquarters staffs and force elements of FMN Affiliates.

c. Operations Planning Environment enables mission partners to collectively share information for operational mission planning and preparation at any time.
The first event to apply the FMN Spiral 1 Specifications in the opportunity to incorporate changes regarding operational missions, minimizes design and development risks, and gives requirements and uncertainty about types and timing of future resolves the problems due to the situation of emerging approaches using spirals. Spirals may overlap. This approach facilitates information sharing.

Implementation

In order to adapt to changing operational requirements, improvements to National FMN Affiliate capabilities, lessons learned and advances in technology, FMN Capability uses an incremental approach to evolve the maturity of the FMN Framework.

In order to implement FMN, the FMN Concept identifies three Milestones that were determined by the information sharing objectives. The three milestones are:

a. Milestone 1 in 2016 aligned with certification of NRF - capability with a maturity level in which separate physical infrastructures exists per mission and per security classification level.

b. Milestone 2 in 2019 - a capability with support for multiple security classification levels within each mission, still with a separate physical infrastructure per mission.

c. Milestone 3 in 2022 - capability with a single common infrastructure for all concurrently existing Mission Networks and their multiple levels of security classification.

To achieve these milestones, FMN Framework Governance and Management organizations proposed an incremental approach using spirals. Spirals may overlap. This approach solves the problems due to the situation of emerging requirements and uncertainty about types and timing of future missions, design and development risks, and gives the opportunity to incorporate changes regarding operational requirements, lessons learned and technology.

The first event to apply the FMN Spiral 1 Specifications in order to build a Mission Network was CWIX (NATO Coalition Warrior Interoperability Exercise) 2014. The goal of this participation was to provide an opportunity to bring Coalition partners together and examine/experiment with their FMN-related capabilities, while assessing the FMN Spiral 1 Specification, and provide recommendations for either further investigation or implementation to improve enablers of theFMN. [5]

Information Management and Protection

Information is the primary resource in FMN concept. Information Centric of Mission Networks is one of the principles stated in the FMN Concept. This means that each MN provides a common mission information domain that facilitates information sharing. Appropriate CIS Security is a derived principle used to guide the direction of the NIFIP. "The FMN and respective elements, federation efforts and systems as well as services are established in a secure way, in accordance with NATO agreed policies and regulations, observing the need-to-know principle while enabling the responsibility-to-share." [3]

A number of communities, changing quickly over time, exist in a mission. Some of them include both mission partners and non-NATO entities.

Information is shared between these communities in a dynamic but controlled manner. Information products can flow to the people that need it while undesirable information flows are prevented and detected. In FMN, CIS Security focuses on the protection of the information itself. This is a different approach to traditional systems were security domains are protected. The security mechanisms has to be strong enough to protect highly classified information and sufficiently flexible to allow effective and efficient information sharing at lower classification levels or at the unclassified level.

According to [3], is defined a model for this approach: Content Protection and Release (CPR) model. This model has some key elements:

- A set of content categories (could be considered a taxonomy) created and maintained to express policy for communities of interest;
- Labelling of information objects, preferably according to the content categories but at a minimum using security labels;
- A protection policy expressing the level of protection that an information object needs to be based on;
- A release policy expressing the level of release based on the content categories and the requirement to share information;
- Release decisions decided upon by correlating the label of the information object, the protection and release policies, and the requestor’s identity, attributes, and ability to protect the information.

Today, NATO provides a practical mechanism for enabling effective information sharing between different entities involved in a mission. In this mechanism, releasing the information to recipients is manually. Soon technology for automated release and multi-level services become available, so the processes become automated. Also, traditional security (or confidentiality) labels move to content labels.

The new proposed standard regarding confidentiality labelling and binding of information take in account the requirements to enable sharing information in a scenario with multiple entities. These entities that are governed by different security policies, wanted to share information based on individual bilateral agreements.

The objective of the standard is "to provide common implementation-independent 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." [4]

According to this standard, the Confidentiality Label includes the following primary elements:

- Governing Security Policy - Security Policy Authority;
- Classification - a single value identifying the classification level of the information;
- Privacy Mark - is used to convey operational instructions, warnings or notifications of significance to the user or custodian of the data object;
- Category - provides restriction and/or expansion of the dissemination within the scope of the classification of the information. The categories are Restrictive, Permissive or Informative. The Category element allows the following subcategories to be defined: Context,
The confidentiality label syntax is based upon the label description from IETF RFC 2634 and includes additional refinements to support requirements for access control for information with a binding mechanism to indicate the confidentiality label that will be applicable at a certain time in the future. The syntax utilizes the eXtensible Markup Language (XML) to represent a confidentiality label. The Confidentiality Label has to be bound by information is labeling. There are three approaches for binding metadata (including Confidentiality Label) with information:

a. Encapsulated labeling - information is separately stored together with the metadata within a container;

b. Embedded labeling - the binding is embedded within the information and the binding contains a reference to the information;

c. Detached labeling - the binding and metadata may be stored in a separate structure from the information with the binding containing an explicit reference to the information.

The information, the confidentiality label and their association need to have a level of assurance and integrity. This level is provided by a Binding Mechanisms. Depending on the level of assurance required the binding go from a ‘loose binding’ (a binding without any integrity protection) to a ‘strong binding’ (a binding that protects the integrity of the relationship, usually created by cryptographic means). Information Assurance means not only confidentiality but also integrity and availability as the intrinsic properties of the information shared. Recently, a STO (NATO Science and Technology Organisation) task group makes new recommendations for the integrity and availability metadata elements to be used by policy rule engines in making decisions on security controls for individual information objects and recognized that there will be challenges in the implementation of these metadata.

National approach
A national approach to implement FMN concept for the Romanian CIS involves two aspects:

a. CIS connected to a NATO MN;

b. CIS connected to a national FMN-based network.

In first case it has to be decided the level of capability we want to choose to contribute to that Mission Network: Mission Network Element, Mission Network Extension or Hosted User. In all situations information sharing is a commitment. The architecture of such systems has to be in accordance with the requirements of FMN architecture as defined in FMN Implementation Plan. Legacy systems need to be evaluated against FMN capabilities in order to provide recommendations for either implementation of such capabilities or improving of the existing. The requirements for new systems have to conform to FMN requirements depending on the highest level of capability wanted for that system.

In order to be able to share information in a NATO Mission Network, a system has to implement a labeling and binding mechanism according to NATO requirements. As the requirements for this capability are recent, it is obvious that most of legacy systems do not have any labeling and binding mechanism. Even legacy systems with such mechanism do not entirely comply with confidentiality label syntax. These systems need to be upgraded in order to be capable to share information in future FMN mission networks. Both new implementations and the upgrades have to be incremental, so they can cover all requirements as soon as shall be specified by the NFIP.

We proposed incremental approach to implement national FMN-based network. We need also to analyse the possibilities to upgrade legacy systems so they can achieve the proposed capabilities. The increments will be set based on the architecture and according to results of these analyses.
Conclusions

As shown in this paper, the implementation of the FMN concept in Romanian Army involves two aspects:

a. In NATO missions, connection of Romanian CIS to a MN organized according to FMN architecture standards and procedures developed by NATO.

b. Connection of all Romanian CIS, including those of the first category, in a national network according to the principles of FMN concept and a national architecture.

The second issue raises the question of defining national architecture which establishes minimum services required for connecting a CIS in a mission network as well as the information exchange procedures, including here structuring of associated metadata to these information such to ensure their confidentiality, integrity and availability. This architecture must be complementary to NATO architecture to enable participation of the national CIS in NATO missions in order to connect simultaneously the two networks types.

In defining national architecture we can start from NATO architecture. At the national level, defining metadata appears to be a less complicated problem because these metadata must follow the structure imposed by NATO standards for national CIS participating in NATO missions.

Therefore, due to the issue complexity needed to be resolved, the Romanian Army concept implementation is standing and requires participation of a large number of structures in all kind of areas (operational, logistical, technical and research) and from all armed forces (land forces, air forces, navy).

It should be noted that this concept can also be applied to connect the national CIS providing necessary data in crisis situations. In such a network, connected systems are very different, belonging to national security institutions as well as civil or government bodies. As in the military case, we need to define the network architecture as well as metadata structure for information sharing.

Bibliography