"Mircea cel Batran" Naval Academy Scientific Bulletin, Volume XVIII – 2015 – Issue 1
Published by "Mircea cel Batran" Naval Academy Press, Constanta, Romania // The journal is indexed in:
PROQUEST SciTech Journals, PROQUEST Engineering Journals, PROQUEST Illustrata: Technology, PROQUEST Technology Journals, PROQUEST Military Collection PROQUEST Advanced Technologies & Aerospace

INFORMATION LABELLING FOR IMPLEMENTATION OF FMN CONCEPT IN ROMANIAN CIS

Lidia BOIANGIU[1]
Diana MILITARU[2]
Bebe-Raducu IONASCU[3]
Madalin GANEA[4]
Stefan POPA[5]
[1]Scientific researcher II, Eng., Military Equipment and Technologies Research Agency, Bucharest,16 Aeroportului Street, Bucharest, 077025, lboiangiu@acttm.ro
[2]Scientific researcher, PhD Eng., Military Equipment and Technologies Research Agency, Bucharest
[3]Scientific researcher III, Eng.,Military Equipment and Technologies Research Agency, Bucharest
[4]Research assistant, Eng., Military Equipment and Technologies Research Agency, Bucharest
[5]Scientific researcher, Eng., Military Equipment and Technologies Research Agency, Bucharest

Abstract: *FMN (Federated Mission Networking) concept was developed in order to ensure global rules for establishing a federation of CISs (Communication and Information Systems) organized in a Mission Network (MN) to "enable effective sharing information among NATO, NATO Nations and/or other NATO / 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.*

Introduction

Future Mission Network Concept was developed in 2012 in response to a request from Military Committee to Allied Command Transformation (ACT) and Allied Command Operations (ACO). The concept was based on "the best practices and lessons learned from the implementation of the Afghanistan Mission Network (AMN)". [1]

With approval of first version of FMN Implementation Plan (NFIP) the acronym FMN was as Federated Mission Network, to reflect the need for 'federation' as the means to achieve full benefit of information sharing.

Overarching guidance is needed to establish a federated Mission Network capability that enables effective information sharing among entities participating in operations (NATO, NATO Nations and/or Non-NATO). The aim of FMN is to provide this guidance. It describes the operational requirements, principles, and implementation considerations for this capability, including the governance, processes and procedures to support command and control (C2) from Headquarters in a federated coalition environment.

The concept reflects the operational experience (from AMN, KFOR, SFOR, etc.) which demonstrated that a federated mission network is the best means to create a common, mission-wide data and information sharing environment.

FMN state of the art

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.

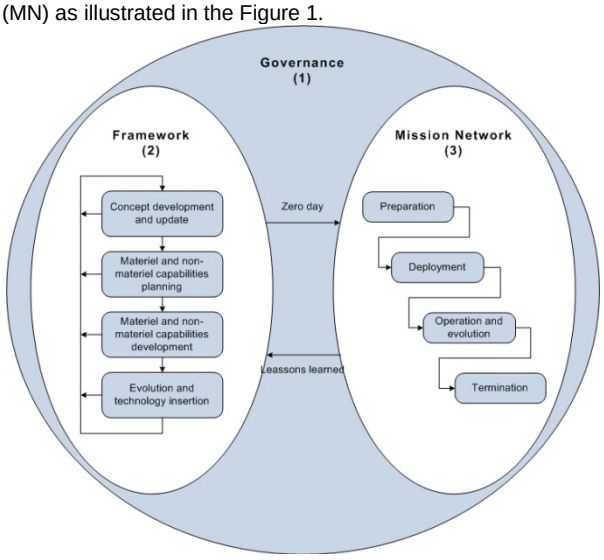

Figure 1.Components of FMN capability (according to [1])

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 Environmentenables mission partners to collectively share information for operational mission planning and preparation at any time.

d. Mission Execution Environment enables mission partners to connect their pre-validated infrastructure to form a federated Mission Network. All interconnections will fully comply with the FMN Instructions.

Levels of capability

The FMN concept defined four graduated levels of capability. These levels provide options for the participation in Mission Networks in particular with regards to the commitment of effort and resources that FMN Affiliates can choose to contribute to any particular mission.

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.

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 resolves the problems due to the situation of emerging requirements and uncertainty about types and timing of future missions, minimizes design anddevelopment 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]

According to FMN Engagement Calendar 2015, changes and new developments shall be tested at CWIX 2015.

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 NFIP. "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 have 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. A set of content categories (could be considered a taxonomy) created and maintained to express policy for communities of interest;
b. Labelling of information objects, preferably according to the content categories but at a minimum using security labels;
c. A protection policy expressing the level of protection that an information object needs to be based on;
d. A release policy expressing the level of release based on the content categories and the requirement to share information;
e. 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:

a. Governing Security Policy - Security Policy Authority;
b. Classification - a single value identifying the classification level of the information;
c. Privacy Mark - is used to convey operational instructions, warnings or notifications of significance to the user or custodian of the data object;
d. 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,

Releasable To, Only, Additional Sensitivity, Administrative.

The confidentiality label syntax is based upon the label description from IETF RFC 2634and includes additional refinements to supportrequirements for asuccession handling for disposition and retention(a mechanism to indicate the confidentiality label that will be applicable at a certain time in the future). The syntax utilises the eXtensible Markup Language (XML) to represent a confidentiality label.

The Confidentiality Label has to be bound by information is labelling. There are three approaches for binding metadata (including Confidentiality Label) with information:

a. Encapsulated labelling - information is stored together with the metadata within a container;
b. Embedded labelling - the binding is embedded within the information and the binding contains a reference to the information;
c. Detached labelling - 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 labelling 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 labelling 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 al requirements as soon as shall be specified by the NFIP.

Much of the objectives identified by the concept can be undertaken at the national level not only for a particular mission but also for daily activities, such:

a. Seamless human-to-human communication across the force;
b. Provision of consistent, secure, accurate and reliable mission data;
c. Community of Interest (COI) capabilities that align with the mission requirement.

So we propose all national systems to be connected to a FMN-based networkin order to be capable to share information in time at all levels of command.

This required the establishment of specific network architecture in accordance to Romanian C2 system. All CIS systems participating in NATO missions should be part of this network.

The second feature that systems of this network must fulfill refers to the protection of sharing information.

As in case of FMN Mission Networks, we need to implement a security mechanismfor enabling effective information sharing between different systems. This mechanism may be similar with NATO mechanism, but there may be some differences. One of these differences is the structure ofthe confidentiality label, which depends on national security policy.

An important aspect in CIS system participating and in NATO missionsis the need for them to implement security mechanism for two security policies: NATO and national. This requirement is clearly stated in NFIP.

In order to bind the two confidentiality labels with the same information simultaneously, we may use more methods:

a. Combining the two labels in one label and using of any of the three approaches for binding metadata with information. This method could create some problems in the accreditation process for FMN.
b. Different labels using two metadata registries, one for NATO policy, one for national policy. In this case we can use only detached labelling approach to bind metadata with information. Despite its complexity, the method is more reliable in terms of the implementation of two policies.

We proposed incremental approach to implement national FMN-based network. We need also to analysethe 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 CISto 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 enableparticipation 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

[1] IMSM-0390-2012, "Future Mission Network (FMN) Concept," NATO, 23 Aug 2012
[2] IMSM-0412-2014, "NATO Federated Mission Netork Implemetation Plan (NFIP)," NATO, 15 September 2014.
[3] 6300 TSC FCX-0010/TT-140129/Ser: NU 0929, "NATO FMN Implementation Plan Version 4.0," NATO, 30 September 2014.
[4] ADatP-yy, "Confidentiality Labelling and Binding for Joint Coalition Information Sharing Edition A Version 1," NATO Standardization Organisation (NSO), September 2014.
[5] 6300 TSC FCX-0010/TT-140099/Ser: NU 0830, "CWIX 2014 Final Report Volume 1," NATO, 9 September 2014.