sciendo

Scientific Bulletin
Vol. XXIV, No 1 (47), 2019

INTERPRETING THE INTEROPERABILITY OF THE NATO'S COMMUNICATION AND INFORMATION SYSTEMS

Szilveszter SZELECZKI
Szeleczki.Szilveszter@uni-nke.hu

NATIONAL UNIVERSITY OF PUBLIC SERVICE, BUDAPEST, HUNGARY

ABSTRACT

In our current network-based world, cooperation between different participants in all areas, for example political, defense, economic or cultural, has an increasing role. Because of this the importance of interoperability between participants is also increasing. The central presence of information also highlights the concept and influencing factors of interoperability. The participants can be individuals, organizations or other groups, where a comprehensive flow of information and the constant presence of the information space is essential for its effective and efficient activity. Interoperability issues are also a key component of the military transformation process of NATO, so basic information questions should be answered to achieve the target system. Nowadays, interoperability requirements and definitions are subject to periodic changes in order to facilitate high-tech joint exercises using advanced technology.

KEYWORDS:

Cooperation, network, interoperability, information, NATO

1. Introduction

In the most military applications interoperability issues became a matter of interest in the 1950s, and later in the 1970s, non-military applications were also of interest. Interoperability, as a concept, can be defined as a complex, everyday interpretation: The ability of different IT (Information Technology) systems to collaborate, where collaboration can take place at different levels and layers. Technically speaking, interoperability between systems is physically possible, and information from one system to another can be interpreted by the person using the system. Interoperability of such a level is the universal services of the internet (e.g.: e-mail, web) are for us. At the level of technical interoperability, we do not deal with the seemingly fundamental problem that data sending and receiving (people may speak different languages). At the level of interoperability taken from semantic approach it is not only physically possible to exchange data, but also to be able to interpret each other's data. This concept means that the data generated in the sending system is transferred to the receiving system in such a way that the receiving system can perform the same operations as if the data were generated in the receiving system itself. During this process, the users

DOI: 10.2478/bsaft-2019-0011

of the system can fully use the data further. Being aware of these two approaches, it is worth pointing out, however, that interoperability is only referred to as the data recorded and managed by the organization in question for its own purposes. We do not use the term interoperability in the case where the data is prepared in advance for the purpose of transmission (e.g.: reporting), and the transmission takes place in a predetermined, bound format. Implementing interoperability is a major challenge, mainly across national boundaries, but with the advancement of time (e.g.: in relation to NATO, North Atlantic Treaty Organisation), it is increasingly necessary to fully develop and mine it. Figure 1 shows the structure that includes the strategic advisor and proponent of NATO, which, with the passage of time, gradually represents a higher standard. It can be seen that interoperability is a distinct, significant component, and therefore plays an extremely important role in the functioning of NATO at all times.

Figure no. 1. NATO's strategy
(Source: NATO, *Mission*)

2. Theory of implementing interoperability

Determining interoperability functions and tasks between IT systems is the requirements for information exchange. These define the basic characteristics of the rules of data exchange (both received and transmitted) between two or more systems, for example what information, what content and in what form and by what rules it should happen.

In the NATO basic and other concepts there are three levels of interoperability, "*namely compatibility, interchangeability, and commonality*" (Munk, 2002, p. 6). These levels illuminate the expected operational layers of interoperability.

2.1. Recognizing the complete interoperability issue

In the exchange of information between IT systems, the problem may arise when the information provided by the current systems regarding the requirements for the exchange of information is not available or is not equivalent, and even if those systems do not have the information at their disposal, they are not capable of the same order, or may not be able to use the information in the same representation.

During the exchange of information between IT systems, problem may arise when the information provided by the current systems regarding the requirements for the exchange of information are not available or are not interpreted in the same way, or if those systems are not capable to use them, or to use them in the same way, or to use them in the same representation. The lack of required information to be processed for the purposes of the affected systems cannot be considered as an interoperability problem, assuming that there is a real co-operation and information exchange requirement between the application fields supported by IT systems.

This case means that the IT systems in question do not adequately support the fields of application concerned. The problem can only be solved by modifying the substantive, fundamental purpose of the given IT system, during which the acquisition or production of information and the utilization or processing of the incoming information must be ensured.

We are not talking about an interoperability problem if the obstacle is the lack of info communication capabilities for the transmission or reception of information involved in the exchange of information. Generally, this can be fixed by incorporating other information exchange functions and the system components that implement them, without substantially altering the basic purpose of the given IT system. Of course, the implemented new capabilities, the order of information exchange, its content and format should be adjusted in accordance with the known information exchange requirements.

From the above, we can speak about interoperability problems when the information stored and managed by the IT systems include the information specified in the information exchange requirements, and that these systems are able to transmit and receive these information, but there are differences in the interpretation, rule of information exchange, or the content or form of representation of these messages. Figure no. 2 shows a kind, symbolized activity, as an example of two NATO member states also seeking cooperation, finding its fast, purposeful way.

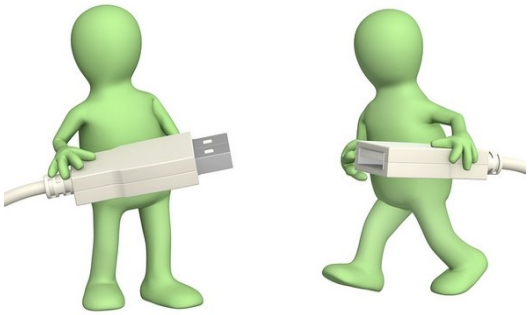

Figure no. 2. Symbolized interoperable cooperation
(Source: Shilovitsky, 2014)

2.2. System theory of information exchange

If there are discrepancies between the IT systems involved in the exchange of information in the area, the following functions and tasks may be required to be implemented to achieve interoperable information exchange:

– to resolve the differences of semantic framework, adjustments between different conceptual systems, semantic representations;

– to resolve the differences in the order of exchange of information, to reconcile an coordinate the protocols necessary for the exchange of information;

– to resolve the differences in syntactic representations, for transformations between different syntactic representations;

– to resolve the differences in material, for example the physical representations for transformations between different material representations.

In order to achieve a preserving receivement corresponding to the information sent by the sender IT system, generally it is not enough to receive only the representations bearing the information. sometimes there is a need for additional components, i.e.

knowledge and information in order to achieve a full-scale, complex cooperation based on same-level interpretation. This pieces of knowledge exist at different levels, both on the document-like and on the narrower sense of the data-like representations. For example documentary representations are text documents in general, but also representations of different map objects may be included.

Data-like representations are those representations whose elementary components are object-specific values, or object-to-object representations, or data elements. Different databases and formatted messages belong in here. Databases and formatted messages might structure themselves into a set of data elements, in which the structures themselves have an appropriate meaning. By using symbolic words, the example of the structural expression, the construction of sentences from words and the sentence structure itself is a key factor in the meaning of a sentence. Thus, the interpretation of the elementary components and the structure itself must be ensured during use. Data elements in themselves are not generally suitable for reproducing the transmitted meaning. Interpretation usually requires knowledge of other data elements.

2.3. The concept of context

When interpreting data from a given source, the aggregate concept of the required components is commonly referred to as context. In this unique interpretation, the context is nothing other than the sum of all the components that are needed to get to know the meaning of the data elements and data sets that make up the information, in other words, the information representation.

These components are concepts, facts, assumptions, and rules. According to a certain wording, "*the context of a piece of data to be the metadata relating to its meaning, properties (such as its source, quality, and precision), and organization*" (Sciore, Siegel & Rosenthal, 1994, p. 2). The components needed to interpret information representations can be divided into different groups:

– "*the technical level of physical media used in the exchange of information;*

– *the syntactic level of the language, message and data formats used;*

– *finally, the semantic level of the content and meaning to be transmitted*" (Munk, 2018, p. 3).

The semantic components represent the data elements and data sets of each representation and their meanings. The basic component of these context components is the conceptual system used by that source. This system describes what objects and their properties and relationships belong to the interests of a particular system, as well as determines the knowledge and information that can be formulated in the given system.

The semantic context components include the interpretation of the individual data elements on its own, and the realization of the reproduction of the report carried by the applied data structures. The meaning of some data elements or batches of elements may not be defined by the context components alone. It may be necessary to include the content of other data elements of the given data set, the data elements previously acquired, sent or received during the acquisition of information, the content of data sets, the circumstances of the information exchange, the factors influencing the circumstances.

Components collectively referred to as a local context may be the same as components of the global context, but of course their validity is limited to the current data set, the complete information exchange process, or the associated circumstances. The syntactic components refer to the formal characteristics of the given representation. This may include information about the used set of symbols, the structural and other syntax rules.

2.4. Interopable tranformation

The notion of contexts needed to interpret information and information representations in the exchange of information can also be used to investigate and implement effective, meaning- and value-preserving information exchange between systems.

Converting from a representation in a sending system to a representation in a receiving system means conversion between different contexts. To successfully complete the transformation, three different groups of components needed:

– a source for the components of a system providing information;

– components of the receiving (information user) system;

– components for system to system transformations.

Of course, contexts and transformation components have to be available in a suitable form to implement the conversion to a specific component, thus implementing the information exchange. The components needed to implement an interoperable exchange of information can be divided into two broad categories:

– application-level interoperability components;

– implementation technical level interoperability constituents.

The implementation of both groups is the responsibility of IT professionals. The application-level group includes those components that are specifically intended for professionals in a particular field of application, such as different semantic components. In the implementation-level group, we can mention the knowledge and abilities such as syntax and technical information.

3. NATO's interoperable ideas

NATO's military operations are carried out in a military, joint, multinational alliance. In order to facilitate the battle groups to successfully accomplish their mission, they must establish an ever closer bond and cooperation among themselves, taking even the different organizational levels into account, such as non-government and civilian organizations. The operation of a given system can only be characterized by full, functional interoperability if it performs accordingly to the requirements and purpose of the co-operation of different levels, thus the exchange of information can be fully accomplished.

3.1. Initial ideas

NATO has adopted several new documents at the 1999 Washington Summit, which was already nearly 20 years ago. It is important to mention the document issued about the challenges and opportunities of the next century as the new Strategic Concept (NATO, 1999, p. 47-60). This document sets forth the following requirement for Alliance forces: "*Alliance forces must be adequate in strength and capabilities to deter and counter aggression against any Ally. They must be interoperable and have appropriate doctrines and technologies*" (NATO, 1999, p. 56). The concept also put a strong emphasis on the key role of interactions between Allied forces and the civilian environment, as well as the political and military benefits of using multinational clusters based on the CJTF (Combined Joint Task Force) concept. It has also been declared that increasing interoperability and organizing appropriate joint training and exercises are of great importance for the full provision of multinational groupings.

Interoperability, including the human factor, the appropriate advanced technology, the maintenance of information applications for superior purposes in military operations, and the presence and development of trained personnel with a wide range of expertise will be very important for their development. In addition to this new Strategic Concept, NATO has published another document entitled as Defence Capabilities Initiative (NATO, 1999, pp. 61-62). In this document,

it is stated that "*The objective of this initiative is to improve defence capabilities to ensure the effectiveness of future multinational operations across the full spectrum of Alliance missions in the present and foreseeable security environment with a special focus on improving interoperability among Alliance forces, and where applicable also between Alliance and Partner forces*" (NATO, 1999, p. 61). Concerning future NATO operations, it is predictable that they will be conducted in smaller scale, but will be longer, extending multinational cooperation to lower levels, and being implemented in parallel with other allied operations.

The initiative focuses on interoperability. As a result, new demands are made on the necessary capabilities of Allied forces, especially on the increasingly important military area, interoperability. Amongst other issues, the initiative states that in the context of Allied forces, "*Command and control and information systems need to be better matched to the requirements of future Alliance military operations which will entail the exchange of a much greater volume of information and extending to lower levels than in the past. Maintaining the effectiveness of multinational operations will require particular attention to the challenges of interoperability. In this context, increased attention must be paid to human factors (such as common approaches to doctrine, training and operational procedures) and standardisation, as well as to the challenges posed by the accelerating pace of technological change and the different speeds at which Allies introduce advanced capabilities*" (NATO, 1999, p. 61).

Prior to the NATO Summit in Prague, defense ministers determined four areas of key operational capability, one of them being the need for improving the interoperability of the forces involved. Later, at the 2002 summit, NATO announced its transformation program, including transformations such as: the transformation of the command structure, the establishment of the NRF (NATO Responce Force) and the declaration of a commitment to establish certain military capabilities (NATO, 2003, pp. 72-74). A functional headquarter has been established in Norfolk, USA. The purpose of ACT (Allied Command Transformation) is to continuously transform military capabilities and to facilitate the possibility and develoopment of interoperability. In 2003, the leadership of NATO created a commitment to capability development in Prague as a result of the failure to implement many of the factors described in the Defense Capabilities Initiative, which consisted of a set of deadlined objectives. Within the framework of the transformation program, great emphasis has been placed on counter-terrorism processes, and the consequences of the terrorist attack of 11 September 2001, as well as recent NATO operational experience, have been analised (Barry, 2003, pp. 1-4).

One of the key elements of the long-term allied vision is the approach of military operations as a whole, the expansion of its scope, information, economic, social, legal, diplomatic, etc activities. Another important element of this vision is the change in the composition of the forces carrying out military operations and the extension of the scope of cooperation.

NATO C3 (Consultation, Command and Control) systems must be fully interoperable, ie they must be able to work with national systems. Consequently, NATO needs an intensive, significantly enhanced interoperability capability at all levels of NATO C3 systems to provide full support for functions ranging from political consultations to combat tactics. The national systems of the Member States and the partners must also cooperate in order to be able to ensure the rapid, efficient and joint activities of the forces during the exercises.

Interoperability used in operations is a reciprocal ability for effective and efficient collaboration. This ability requires

appropriate level of interoperability in each functional areas, as in leadership, guidance, discovery, logistics, etc. The abilities listed are based on the capability of interoperability in the technical sense, the operational condition of which is the stable interoperability of military IT systems.

NATO attributes the fundamental pillar of the vision to the role of information superiority, and regards the dependency of information systems and modern, state-of-the-art technology as being one of the most prominent areas of the future. In practice, for example the role and importance of sharing intelligence information and establishing common situational awareness will be specifically highlighted in the information flow. Another key component of NATO's vision is the network-centric approach that is playing an ever-increasing role in these ideas, this is so-called as NNEC (NATO Network Enabled Capability). Some components of the vision have also been analysed in military science literature (Binnendijk, Gompert & Kugler, 2005, p. 5). The allied structure and development of interoperability is generally influenced by the varying IT development of each NATO member state's army, their specific national requirements, and the operation of the NATO reconciliation mechanism.

3.2. NNEC in the future

The NATO C3 Board decided in 2002 to introduce a new approach, the establishment of NNEC. For commanders, the issue of network-based capability appears as a basic requirement factor. Network-centric capability includes all systems involved in the operations, whether let it be weapon systems, different sensors, other means of communication, or a link between governmental and the non-governmental institutions. The capability also includes design, evaluation, and other implementation roles. Network-based capability must ensure the timely exchange of protected information. Existing info communication networks, which are interoperable and require stable operation according to their requirements, should be used in the implementation and should also support the collection, analysis and of course, sharing of information (Farkas & Hronyecz, 2017, p. 356).

In order to start the implementation properly, NATO experts have begun a very thorough preparation based on assumptions and evidences. The NATO Feasibility Study, issued in October 2005, is linked to this. It is undoubtedly not a question that the development of network-centric capability has a major impact on the implementation of interoperability solutions.

According to that study, three activities needed to implement network-centric cooperation. "*Firstly, there is the need to extend communication networking capabilities to 'wherever they are needed, whenever they are needed', implying the need for a 'flexible global networking capability'. Secondly, there is a need to support smaller, modular, multinational force structures such as the NRF, generating new information-sharing and security requirements that will increase critically of interoperability requirements and could redraw NATO/national interoperability boundaries. Thirdly, there is the need to support the rotation of national force elements within the NRF and to support seamless interoperability with force elements from non-NATO nations that may not even be identified until a mission is already underway. These points imply the need for an unprecedented degree of flexibility, agility, adaptability and interoperability in the force structures involved and in the networking and information systems that support them*" (NATO, 2005, pp. 2-3).

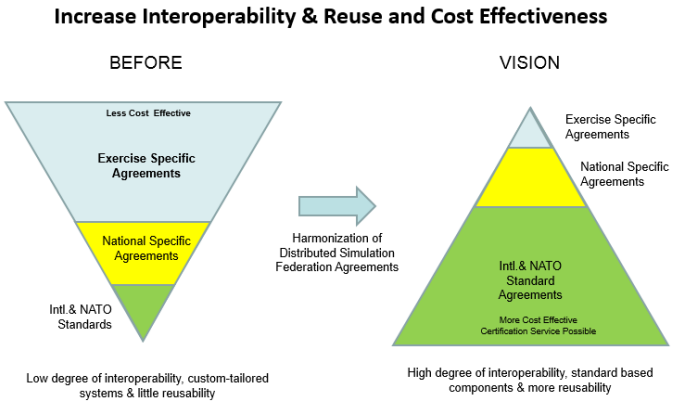

Figure no. 3. Effectiveness of NATO interoperability
(Source: NATO, *Establishing a HLA certification process in NATO)*

Figure no. 3 shows a NATO logical vision of how cooperation between member states can change and what they gain if they concerning the future – for example put more emphasis on improving interoperability problems. Network-centric warfare can have a great impact on the efficiency and operational quality of a so-called networked force. In the newest division, this strategic system defined as FMN (Federated Mission Network). Here, information sharing as a basic function can greatly improve the performance of an operation. Among the information, the awareness of positions own and hostile forces is outstanding, and the possibility to evaluate the qualities of other given locations without for example having to observe it visually from a sufficient distance.

The information availability helps to increase the capability of joint operations and its effectiveness. Better situation awareness increases the sustainability and the speed of the operation. The network-based capability mentioned above is in terms of architecture mainly comparable to the GIG (Global Information Grid) architecture:

– the user layer;
– functional applications;
– information and integration services;
– communication services;
– system and network management, information security.

NATO's network security is based on NII (Network and Information Infrastructure), building on the mass of interoperability issues and tasks. The communication infrastructure is based on the widespread application of IP (Internet Protocol). Sound, video and data traffic with different classifications is managed by the so-called "*black*" core network, NATO's unified virtual network operating on an open level. "*FMN Capability enables to connect forces in a federated mission environment at any time, in a short period of time and at an optimised level of interoperability*" (NATO, 2016, p. 10).

The basic condition for its implementation is the installation and smooth application of interoperable IP encryption tools. The purpose of information and integration services is to provide information resources and services on the network, to find and use them with an effective and confident impression of the current user. The key issue of information interoperability between NATO member countries is meta-data standardization, creating specialized dictionaries. The purpose of the information security component is to ensure that information is passed on to the right users at the right time. The other main task of information security is that the quality of the data sent cannot be impaired in the displayed syntactic interpretation.

The development of a network-centric information infrastructure is based on the interconnection of NATO member states networks and IT systems. The goal is to achieve FoS (Federation of Systems) as a result of the success of these operations, which is the sum of the various systems.

Systems in this alliance are not centrally managed, but are related and interdependent to provide more and better services than as individual systems. NATO's IT, network-centric, interoperability-related regulatory and support components are organized into a multilayered structure whose name, structure, and elements are going through continuous development and transformation in the 21st century, in order to achieve the goal.

3.3. Organizing the NATO interoperability system

The definition of IT interoperability policy falls within the responsibility of the NATO C3 Board. The purpose of NATO's Policy for C3 Interoperability is to define the core concepts of NATO interoperability and related roles. The purpose of this document is to increase the operational efficiency of the alliance and the efficiency of the use of available resources within the framework of the implementation of interoperable IT systems.

The abbreviated name of the NATO system was originally NIF (NATO Interoperability Framework). This type of system had three layers as politics, implementation, and products. The policy layer was solely made of a document on NATO's IT interoperability policy. The components of the implementation layer were included in the NATO Interoperability Management Plan and the Rolling Interoperability Program. The products layer, also known as the NATO IT Interoperability Environment, consisted of two components to support design and implementation.

Subsequently, the designation of the NATO Interoperability Framework changed and its structure was changed to a four-layer structure. The single component of the policy layer remained and unchanged. The implementation layer became divided into two separate layers. The policy layer is made up of the NID (NATO C3 System Interoperability Directive), while the guidance layer is made up of the IT system transformation interoperability manual, that is so-called NTIH (NATO C3 System Transformation Interoperability Handbook).

Supporting components include the framework for IT system architectures, the IT technical architecture, interoperability environment testing infrastructure, interoperability tools, and NATO interoperability profiles and regulators. The development of NAF NC3TA (NATO System Architecture Framework NATO C3 Technical Architecture), shown in Figure no. 4, is a still ongoing procedure.

Figure no. 4. NATO C3 Interoperability Environment
(Source: Burita, 2010)

The purpose of the NID is to define the policies to be followed and the mandatory support components to be respected in the NATO NIF, and to define the responsibilities of the participants involved. Among the listed components, the name of NATO's IT interoperability policy has been slightly modified, but its structure remained and unchanged. There has been no significant change in the technical architecture of the NATO IT system, but modernization of tools and IT services standards is still in progress.

4. NATO's effectiveness in interoperability

One of the most commonly used solutions nowadays to the interoperability problems of value-retention of information systems between IT systems is standard-dization, which provides a comprehensive application that facilitates the execution of repetitive tasks.

4.1. Effective exchange of information

Solutions for information exchange may be applied to its different forms, components, or different levels, including:

– rules of information exchange (e.g. different protocols);

– exchange of free-form, semi-standard and standard (formatted) information;

– physical, syntactic and semantic levels of information exchange.

The essence of interoperability solutions based on global or application-specific standards developed on the theoretical level or developed from practical experience is that the ability to apply standard information exchange solutions is the responsibility and responsibility of collaborative IT systems. In this way, an IT system capable of applying a standard for information exchange can theoretically exchange information with any other system featuring supposedly similar capabilities. Where different standard solutions are applied, each system must be able to apply more information exchange solutions in the same collaboration process. In an event of information exchange, standardization solutions can be divided into three groups:

– standards for document format;

– standards for message format;

– data element standards.

Standard document file formats for document-specific information exchange include text, spreadsheet, drawing, or multimedia document formats. These standards define the format of documents having various content, transmitted between IT systems. For a given document type, there are usually many different formats used in practice, so one has to choose the preferred version or variations. The message format standards can be divided into two large groups consisting of bit-oriented and character-oriented message standards. The two types meet different needs and partially use different solutions. The purpose of bit-oriented message standards is to support time-critical, real-time information exchange in military information technology. Examples are weapon control and weapon systems. The purpose of character-oriented message standards is to support the exchange of less time-critical information in military applications such as exchange of information between headquarters.

Contrary to the previous two types, data item standards focus on the much narrower but not less important area of data exchange between databases, and unification of data elements used in formatted messages. The definition of standard data elements includes everything that defines the content description of the data element, the definition of its values and their format, and its components for a complex data element. "*Information should have standardized structures and consistent representations to enable interoperability, cooperation, and more effective and efficient processes*" (NATO, 2017, pp. 1-12).

4.2. Efficiency in practice

In military practice, the main users of message standards are people who work

more or less in the IT area. Message standards can be formed during design, e.g. solution parameterization of weapon system by actual carrier dependence, special or unique technical solutions, radio communication network design, and special areas.

Of the message standards, the distinctive feature of bitstream standards is that they cover all three levels of information exchange, and control the mode of transmission along with the content and format of messages. The character-oriented message standards in the military application are MTF (Message Text Formats). As opposed to bit-oriented message standards, character-oriented standards do not address the way in which messages are delivered, only the content and format of messages that are applicable to them. Message standards are employed by their users and affected systems in order to develop and maintain situational awareness and to support leadership and management. Their core functions include detection, support (whether of air traffic control, airborne intercept control, airstrike control, landing support), navigation and identification, and connection management. Figure no. 5 shows the latest NATO interoperability system exercise, where cooperation between member states's military systems has been investigated. The streams of data, according to NATO's ideas, must be channelled into the so-called COP (Common Operational Picture) from the apparently different systems.

Figure no. 5. CWIX – Coalition Warrior Interoperability exercise in June 2018
(Source: NATO, 2019)

5. Summary

The operation of IT interoperability system the described above ensures the unified interpretation of the data elements involved in the exchange of information and determines the basis for the implementation of the element-level transformations of data between their own information representations and the intermediary representation. A general feature of NATO's IT interoperability standards is that lower levels are characterized by common, widely used solutions that gradually extend to syntactic levels.

Application-specific solutions basically associated with the semantic level dealing with content issues, since that is what is directly related to the application properties and features, while the underlying levels are essentially only definitions of functional and efficiency requirements. The different levels need to be examined and evaluated in elementary steps to achieve proper functioning, and then harmonising the levels can bring the desired final action which can be required in system-level interactivity-related operation. The emerging integration problems must be systematically reviewed

and a complex formula to be developed in order to solve it.

Maintaining and improving NATO's interoperability is essential for the development of joint military action by member states. "*The primary goal of the FMN capability (= mission networking in a federated environment) is to support command and control and decision-making in future operations through improved information-sharing*" (NATO, 2018, p. 5).

These interoperability features may have a different level of quality in practical IT applications tested on different military arenas (land forces, navy, or air forces) due to the geographical position of a NATO member. Improvement of these is based on common interests and is realized in collaboration. Communication tools among member states are not necessarily the same in terms of interoperability capability, but using common data standards and data models for IT applications can solve all these problems with tactical, operational, leadership and support. The deliberate goal dictates that a given member state must first be able to apply IT interoperability at the same time to the said scene, if possible.

As the result of these, member states should strive for fluency and efficiency in NATO-level system practices and fix problems to be solved by joint effort. Expanding this is a key issue for the interopable vision of cooperation between member states.

REFERENCES

Barry, C. L. (2003). *Transforming NATO Command and Control for Future Missions.* WA, USA: National Defense University Press – Defense Horizons.

Binnendijk, H., Gompert, D. C., & Kugler, R. L. (2005). *A New NATO Military Framework.* WA, USA: National Defense University Press – Defense Horizons.

Burita, L. (2010). Command and Control Information Systems Interoperability in NATO, *Conference ICMT'10-IDEB'10, Vol. 1,* Bratislava, Slovak: TnUAD, available at: https://www.researchgate.net/figure/The-environment-for-achieving-C2IS-systems-interoperability-in-NATO-To-facilitate-C2IS_fig1_288446125.

Farkas, T., & Hronyecz, E. (2017). Info-communication areas of modernizing field C2 systems and command posts in the interest of successful home defense- peace operations- and disaster-management tasks. NY, USA: *IEEE 15th International Symposium on Intelligent Systems and Informatics: SISY 2017.*

Munk, S. (2002). *An analysis of basic interoperability related terms, system of interoperability types.* Budapest, Hungary: National University of Public Service – AARMS.

Munk, S. (2018). *Interoperability Services Supporting Information Exchange Between Cybersecurity Organisations.* Budapest, Hungary: National University of Public Service – AARMS.

North Atlantic Treaty Organisation (NATO). (1999). *The Reader's Guide to the NATO Summit in Washington.* Brussels, Belgium: Author.

North Atlantic Treaty Organisation (NATO). (2003). *The Prague Summit and NATO's Transformation. A Reader's Guide.* Brussels, Belgium: Author.

North Atlantic Treaty Organisation (NATO). (2005). *NATO Network Enabled Capability Feasibility Study. Executive Summary: Version 2.0.* Brussels, Belgium: Author.

North Atlantic Treaty Organisation (NATO). (2016). *FMN for Coalition Operations.* Brussels, Belgium: Author.

North Atlantic Treaty Organisation (NATO). (2017). *Allied Joint Doctrine for communication and information systems.* Brussels, Belgium: Author.

North Atlantic Treaty Organisation (NATO). (2018). *ACT engagement in Federated Mission Networking (FMN).* Brussels, Beligum: Author.

North Atlantic Treaty Organisation (NATO). (2019). *Coalition Warrior Interoperability exercise*, available at: https://www.act.nato.int/cwix.

North Atlantic Treaty Organisation. *Establishing a HLA certification process in NATO*, available at: https://www.mscoe.org/nmsg-134-ivct-integration-verification-certification-tool/.

North Atlantic Treaty Organisation. *Mission.* Brussels, Belgium: Author, available at: https://lc.nato.int/about-us/mission.

Sciore, E., Siegel, M, & Rosenthal, A. (1994). Using Semantic Values to Facilitate Interoperability Among Heterogeneous Information Systems. *Journal ACM Transactions on Database Systems (TODS), Vol. 19, Issue 2*, NY, USA: ACM Digital Library.

Shilovitsky, O. (2014). *IoT and PLM have common problem – data interoperability,* available at: http://beyondplm.com/2014/09/26/iot-and-plm-have-common-problem-data-interoperability/.