VÉDELMI INFOKOMMUNIKÁCIÓ

Prof. Col. SÁNDOR MUNK, PhD

NEW REQUIREMENTS AND SOLUTIONS IN THE FIELD OF MILITARY IT SYSTEMS INTEROPERABILITY

ÚJ KÖVETELMÉNYEK ÉS MEGOLDÁSOK A KATONAI INFORMATIKAI RENDSZEREK INTEROPERABILITÁSA TERÜLETÉN

A katona politikai környezet erőteljesen megváltozott a XXI. században. Az új kihívások új, egységesebb megközelítést követelnek a jövőben az egyéb gazdasági, társadalmi, jogi és diplomáciai kezdeményezésekhez kapcsolódó katonai műveletektől. A jövő katonai erőinek teljesen interoperabilisnek kell lenniük más katonai erőkkel és képeseknek kell lenniük arra, hogy zökkenőmentesen együttműködjenek a civil hatóságokkal, a nem kormányzati szervezetekkel, valamint egyéb ügynökségekkel a közös műveleti területen.

The military-political environment has dramatically changed in the XXI. century. The new challenges require a new, more holistic approach of future military operations linked to other economic, social, legal, and diplomatic initiatives. Future military forces must be fully interoperable with other military forces and capable of interacting seamlessly with civil authorities, non-governmental organizations and other agencies in the joint operational area.

Information, and decision superiority depends on timely and accurate information and the means to securely exchange and interpret it in a commonly agreed way. Interoperability and interconnectivity will be key enablers to achieving decision superiority.

Traditional ways, and methods to achieve interoperability between/ among military IT systems are more and more inappropriate in the new

military information environment. It is necessary to analyse the types, and nature of different IT interoperability environments, develop and assess new methods to ensure interoperability of military IT systems.

Introduction

Prior to the NATO Prague Summit NATO defence ministers, as a preparation of Prague Capability Commitment, identified four key operational capability areas. These included the improvements in interoperability of deployed forces.[1] Operational interoperability is a mutual capability of actors to ensure a successful and efficient cooperation that requires appropriate level of interoperability on different functional areas (such as command and control, intelligence, logistics, etc.). All functional area interoperabilities are based on information interoperability, and technical interoperability.[2]

An essential condition of ensuring all the interoperability types mentioned above is interoperability of military IT systems. According to the basic NATO document on this topic „Common-funded NATO C3 systems must be fully interoperable and must inter-operate with national systems. Likewise, national systems of members and Partners must inter-operate to enable forces to operate together effectively. NATO, therefore, needs considerably improved interoperability across all levels of the NATO C3 System for the support of functions ranging from political consultation to tactical battlefield operations."[3]

In practice, interoperability between/among military IT systems first appeared in case of actors working on similar functional, or professional areas, and being in a permanent, and close cooperation. Traditional IT systems' interoperability solutions, based on standardized protocols and intermediary representations (bit- and character-oriented message formats, common data models), were developed in support of these kind of cooperation. In the changing international security environment, and as a

---

[1] The Prague Summit and NATO's Transformation. A Readers Guide, 2003, 27. o.

[2] See: Sándor Munk: An analysis of basic interoperability related terms, system of interoperability types. In Academic and Applied Research in Military Sciences, 2002/1. sz., 117–132. o.

[3] Draft NATO Policy for C3 Systems Interoperability. 2003, 5. o.

consequence of changes in nature of military operations, and structure of forces, the traditional interoperability solution is less and less appropriate.

Military IT systems must be interoperable no longer only in a limited cooperation area, but in a dynamically changing environment. This requires a new actor-oriented approach of interoperability, and theoretic studies of the concept, and characteristics of interoperability environment. Moreover it is necessary to analyze changes in the interoperability environment of military IT systems.

This publication introduces the concept of interoperability environment, identifies its basic types, and analyses the changes in the military cooperation environment from the point of view of information interoperability.

The concept and characteristics of interoperability environments

Concept of interoperability, and information interoperability is essentially a relational concept. According to the commonly accepted understanding a specific actor, system, device can not be interoperable in itself, but only related to a well-defined group of actors, systems, devices, in cooperation (inter-operation) with them. So information interoperability is a mutual capability of different actors necessary to ensure exchange of common understanding of information needed for their successful cooperation. Similarly IT interoperability is a mutual capability of IT systems, devices, applications to receive, exchange data, preserving the meaning assigned to data by the primary user community.

Questions of interoperability could be studied not only from the point of view of a given community of interest, but from the point of view of the individual cooperation objects. Community of interest oriented approach deals with cooperating objects, the cooperation between them, and the interoperability requirements and solutions during this cooperation. It leaves objects not interested in the cooperation, and other communities, and areas of interest out of consideration. On the contrary actor oriented approach concentrates on the questions of interoperability between a given object and all of his/her cooperating objects, irrespective of the fact, that the given object is in connection with one, or more communities of interest.

Taking the common understanding of the concept of environment as a starting point, information interoperability environment is based on the interoperability relationships of actors, and components of infosphere. Since information interoperability is a mutual capability of actors to exchange information preserving the common understanding, interoperability relations are essentially the same as information exchange relations, because practically in case of all information exchange relation there could arise interoperability problems.

Information interoperability environment can be interpreted from the point of view of a given actor, a group of actors, or in general sense. The basic concept is the information interoperability environment of an actor: the group of those actors with whom the given actor exchanges information, or whose information he/she acquires, and exploits (with or without their permission), and finally the IT systems, devices possessed, and the information handled by these actors.

Information interoperability of a group of actors is the complex of the information interoperability environments of actors forming the group, that is to say all actors, their IT systems, devices, and information, that are in information exchange relation with some member of the group. So we can talk about the information interoperability environment of an organization, an organizational system, or a mission oriented grouping — e.g. a given brigade, a given arm of an armed force, or forces executing a given military operation.

Information interoperability environment can also be interpreted in general sense. This global information interoperability environment is actually the same as the global information environment, since all actors of the infosphere, at least potentially, are in information exchange relation with other actor, or actors (practically there are not any isolated actors on the infosphere).

We can also define the concept of the IT interoperability environment of a given IT system as all those IT systems (devices), that are in direct, without human interaction, information exchange relation with the given system. IT interoperability environment includes information, or rather data carrying these information, handled, or exchanged by the given systems. In the same way can be defined the IT interoperability environment of a group of IT systems, devices. Information, and IT interoperability environments can be classified into three types, these are the elementary, combined, and dynamic environments.

The main characteristic of elementary interoperability environment is that information exchange relations of the given IT system are related to a well defined, permanent, close, functional area cooperation. So interoperability objectives of the given system aimed at developing, and maintaining interoperability with IT systems of members of a well defined community of interest. In the given cooperation group, conditions of IT interoperability can be created by preliminary agreements, the intermediary representation („common language") can be developed, so the appropriate interoperability solution can be realized and continuously maintained.

The speciality of combined interoperability environment is that the given IT system is in connection with more IT systems, that are members of more previously known community of interest, and these communities develop their interoperability solutions independently of each other, or only a partially coordinated way. Number of these communities is usually few, rarely greater than 2-5. These IT systems know, and use intermediary representations of more communities of interest („they speak several languages"). Conditions of interoperability in this case can also be created in advance, the combined interoperability solution for the given system can be previously developed, and continuously maintained too.

In case of dynamic interoperability environment, the given system is in information exchange relation with IT systems of more communities of interest, but the number of communities is significantly higher than in case of combined interoperability environments, and their list is dynamically changing, because some of them appear only in connection with the particular mission (operation). So in contrast with the previous two types, conditions of interoperability can be only partially created in advance, only on the previously known cooperation areas. Interoperability solutions in the dynamically appearing cooperation areas, and relations must be finished, and tailored to the given situation in the course of operations, in the period of preparation, or execution.

The changed cooperation and interoperability environment

The beginning of the XXI. century is characterized by significant changes in the international security environment, the nature of military operations,

the missions, and structure of military forces executing operations, and in doctrinal principles. These changes have definite influence on requirements of interoperability between military IT systems, and on possible ways, and methods of ensuring interoperability. In the following we will analyze and summarize the most important changes has happened (or will probably happen), and their consequences. For this purpose we will take the common vision of the two NATO strategic commanders as basis.[4]

One of the basic element of the allied commanders' strategic vision is the holistic approach of military operations, and the extension of their relations to other — informational, economical, social, legal, and diplomatic — activities.[5] This involves significant extension in, and continuous development, and changes of information used in preparation and execution of operations.

Other significant element of strategic vision is the change in structure of forces executing military operations, the extension of the circle of cooperation partners, and the evolving dominance of multilaterality. Military operations of our age are planned and executed in a joint, combined — allied, and even coalition — framework, usually established for the given mission, and based on occasional national offerings. Moreover to fulfill their mission the executing forces must establish close cooperation with other, non-military — international, governmental, non-governmental, and civil — organizations.[6]

From the changes, and characteristics presented before it follows that a given military organization, and its IT system(s) should exchange information with a lot of such other organization and IT system, with whom previously it had no, or only partially had opportunity to come to an agreement, and to create the necessary conditions of information, or IT interoperability. The range of potential cooperation partners spans from the units of the own arm, or own armed force, through the allied, or coalition organizations, to most diverse organizations. At the same time this scale demonstrates the differences in interests, in the closeness of cooperation, in the level of autonomy, and as a consequence in the amount, and characteristics of information exchange relations.

---

[4] Strategic Vision: The Military Challenge (By NATO Strategic Commanders). NATO, 2004.

[5] Strategic Vision: The Military Challenge. Points 11., 13., 18.

[6] Strategic Vision: The Military Challenge. Points 17., 21., 22., 23.

The strategic vision emphasizes the role of information superiority, as a fundamental factor, and the dependence of organizational success on the extensive, and efficient application of information, information processes, information systems, and the services provided by information technology. In the document particularly points out the role, and significance of information (in the first place intelligence) sharing, and creation of situational awareness.[7] The consequence of this statement is the continuous development in the exploitation of IT systems, applications, and information handled by them, and in the amount of information exchanged between IT systems of different actors.

Finally one of the most stressed component of the NATO commanders' strategic vision is the emerging network oriented approach, that plays a significant role in doctrinal ideas or our age, and its NATO concept, the network enabled capability.[8] Both on organizational, and system level this approach essentially requires an ability to interconnect with other components on a mission-oriented way, to synergically complement each others capabilities, and an ability to efficiently adjust, adapt, and self-reconfigure to a dynamically changing environment.

According to commonly accepted understanding, network centric force is based on the networking of sensors, gathering information; systems, and devices used in mission execution, exploiting information; and command and control systems, and tools supporting organizational level information processing (analysis, evaluation, and decision). This extremely increases information (data) exchange requirements mainly on the level of technical systems, and devices. According to network oriented approach a given IT system should be able to exchange (or acquire) information with (from) existing, and newly appearing systems of a cooperative, neutral, and even adversary actors of infosphere.

As a summary it can be stated, that ideas formulated in the NATO strategic vision describe, outline, and prognose such an information interoperability environment, where:
  ➢ conditions of information, and IT interoperability should be ensured for a dynamically extending, and a mission-oriented way changing circle of actors of the international security sphere;

---

[7] Strategic Vision: The Military Challenge. Points 14., 18., 31.
[8] Strategic Vision: The Military Challenge. Points 29., 32.

> ➢ amount of information handled by the individual actors, and exchanged between them is continuously increasing, its content is dynamically changing;
> ➢ more and more increasing part of information appears in IT systems, and is exchanged between them, and in a significant manner extends the amount of connections between IT systems.

All these facts naturally influence the quantity, content, and inner representations of information handled by military IT systems, and the quantity, content, and intermediary representations of information exchanged between IT systems.

Summary

Concept of interoperability, according to the commonly accepted understanding, is a mutual capability of different actors, systems, or devices necessary for successful cooperation. In the new Information Age one of the fundamental types of interoperability is information interoperability, and its increasingly important subtype is interoperability of IT systems (IT interoperability). Questions of interoperability could be studied not only from the point of view of a given community of interest, but from the point of view of the individual cooperation objects.

Due to the continuously developing IT support, the realization of information functions, and activities with the help of IT systems, and as a consequence the extension of connections between IT systems, the significance of actor oriented approach of interoperability has grown, and introduction of concept of interoperability environment, and analysis of its characteristics has became necessary.

Interoperability environment of an IT system is the set of all those IT systems (devices), that are in direct, without human interaction, information exchange relation with the given system. Based on amount, and permanence of connections between systems we can distinguish the elementary interoperability environment (when information exchange relations of the given IT system are connected to a well defined, permanent, close, functional area cooperation), the combined interoperability environment (when the given IT system is in connection with IT systems of more, previously known community of interest), and the dy-

namic interoperability environment (when information exchange relations are dynamically changing, and some of them appear only in connection with the particular mission/operation).

In case of military IT systems, in our days, characteristics of their interoperability environment are basically depend on the significant changes in the international security environment, the nature of military operations, the missions, and structure of military forces executing operations, and in doctrinal principles. As a result, amount of information handled, and exchanged by IT systems, and amount of information exchange relations between systems are significantly increasing.

REFERENCES

Draft NATO Policy for C3 Systems Interoperability. NATO, 2003.

Sándor Munk: An analysis of basic interoperability related terms, system of interoperability types. In. Academic and Applied Research in Military Sciences, 2002/1. sz., 117–132. o.

The Prague Summit and NATO's Transformation. A Reader's Guide, NATO, 2003.

Strategic Vision: The Military Challenge (by NATO Strategic Commanders). Allied Command Transformation, Allied Command Operations, 2004.