AARMS
Vol. 3, No. 4 (2004) 527–540

Role of semantic interoperability in warfare of our age

SÁNDOR MUNK

Department of Informatics, National Defence University Miklós Zrínyi, Budapest, Hungary

In the world of globalisation the cooperation between/among different actors plays a more and more important role in every sphere. On the basis of this, the importance of the interoperability grows continually. This is particularly true for information interoperability that has three levels (physical, syntactical, semantical). This paper analyses the growing importance of cooperation, and information exchange, introduces the basics of information interoperability, and examines the connections between information interoperability and emerging concepts of information age warfare. Finally it presents a definition of semantic interoperability, and gives reasons for further discussions.

Introduction

In our world of globalisation the cooperation between/among different actors in every sphere (political, defence, economical, cultural, etc.) plays a more and more important role. On the basis of this the importance of interoperability between these actors grows continuously. In addition, the evolution of Information Age has as a consequence the increasingly growing importance of information interoperability. Nowadays successful and efficient activity, or operation of actors (individuals, organizations, systems) essentially unthinkable without extensive information exchange between actors, and without widespread use of different information sources, information services of the infosphere.

Information exchange with other actors of the infosphere, and utilization of available information services have an important role in development and maintenance of information superiority (advantage), and in consequence of operational superiority (advantage) in conflict, and competitive situations, and in increase of operational effectiveness in neutral environments. A given actor can enhance its functional capabilities, operational effectiveness by, among others enhancing of its information capabilities. The two possible ways are: to enhance the individual (inner) information capabilities, and to increase the efficiency of the information relations, interconnections with the cooperating, neutral, and adversary environment.

Received: April 22, 2004

Address for correspondence:
SÁNDOR MUNK
Miklós Zrínyi National Defence University
Department of Informatics
P.O. Box 15, H-1581 Budapest, Hungary
E-mail: munk@zmne.hu

Information interoperability necessary for information exchange between actors, and utilization of information resources can be divided into different components, into different levels. In the literature it is commonly accepted a three-level system. The first is the physical (material) level of representations, mediums used in information exchange, and information gathering; the second is the syntactical level of languages, message- and data formats; and the third is the semantic level of content, and meaning to exchange. A paper discussing the issues of C2 interoperability is also based on these levels (DRIESENAAR, 2001).

Cooperation, information exchange, information interoperability

The reason for the appearance and increasing importance of interoperability – as an essential capability to develop – in security policies and doctrinal documents is on the one hand due to the, in some respect, increasing heterogeneity of military forces, and groupings in different areas and to different degrees, and on the other hand to the extended possibilities of information exchange and information access based on the accelerated progress in the field of information technology.

Cooperation, interoperability, heterogeneity

As a preliminary approach, issues of interoperability, and specially information interoperability will be discussed in the framework of operations, the complex systems of activities carried out to accomplish a given mission, under unified command and control. Successful execution of these – military, disaster relief, humanitarian assistance, etc. – operations requires strong cooperation of the participating actors (organizations, persons) with different capabilities, and coordination of their activities. This does not mean, that in the case of smaller, less complex activities carried out by smaller, and more homogeneous forces necessity of interoperability has no any sense, but obviously its significance is smaller, its implementation and maintenance is simpler.

Organizational level – operational – interoperability requires an appropriate level of cooperation capability of the actors in each functional area of their activities. Since an adequate organizational level cooperation is impossible without the required level of coordination of the appropriate organizational functions (functional processes). Different functional area interoperability types have different significance. The primary role by all means belongs to command and control (C2) interoperability, because the C2 processes create and maintain basic conditions of cooperation between actors. C2 interoperability is a mutual capability of actors to ensure linking of their command and control processes, harmonization of common goals and situational awareness, and coordinated planning and execution of the necessary activities.

C2 interoperability requires regular exchange of information (i.e., communication), and as a base for this, common, shared knowledge components (system of concepts, pieces of knowledge, etc.). There are also other related concepts, such as language interoperability, conceptual interoperability, or intellectual interoperability. These can be realized by harmonizing doctrinal principles, the mutual knowledge of the procedures used in different armed services, and national armed forces, that can evolve and be consolidated only in practice, in case of military operations only in the course of joint and multinational exercises.

Heterogeneity of forces conducting operations exists in many different areas, and a lot of them are unavoidable. The first and most fundamental type of heterogeneity comes from the differences based on the division of labour, the field specialization that is an inherent characteristic of large organizations, organizational systems. In the case of armed forces, the field specialization appears in the form of armed services, and arms.

The next version of heterogeneity appears in the differences in technical systems, and equipments of organizations, organizational elements with same functions. Units equipped with different technical means, but with identical main functionality have, to some extent different capabilities, their state can be described with partly different information, in order to fulfil their tasks they require partly different information. These differences demand specific requirements concerning the apriori knowledge of these organizations, and the contents and form of the information exchange done with them.

Heterogeneity in equipments is mostly natural, and mostly unavoidable. The reasons lie in the specialties of the technological development, and in the requirements of organizational effectiveness, and economy. Theoretically it is not impossible to equip all the organizations with same functionality with the same, brand new technical systems, but this is nor necessary, neither economical. In addition to train and exercise for use of these equipment is time-expensive, and costly. As a consequence, even in the armed forces with greatest financial resources different equipments of different generations live together.

A third version of heterogeneity is in the execution of tasks, and in the procedures and methods applied by organizations with the same functionality, and equipment. These differences arise from the variances in the superior environment (doctrines, directives, regulations, etc.), the personal qualities and attitudes of the members of the organization, and the organizational traditions, cultures. This leads to the realization of the emerging significance of national, and cultural differences, and to the questions of combined joint operations.

Heterogeneity of forces conducting military operations

Nowadays, in case of forces conducting military operations, and in consequence of increasing importance of multinational operations, degree and role of heterogeneity forms discussed above have essentially grown. Continually growing heterogeneity – among others in doctrines, training levels, technological levels, or cultures – is one of the basic features of 20th century warfare, and recent military operations. Roots of this process can be found in the third part of the 20th century, and the reasons of its acceleration are the essential changes occurred in the threats, and challenges requiring military responses, and in the security environment.

On the security scene of our days basic forms of management of emerging crises, defence against security threats (terrorism, proliferation of weapons of mass destruction, illegal transfer of arms), disaster relief, or humanitarian assistance are solutions based on cooperation of nations concerned in preservation of global, or regional security. This is equally holds in case of operations conducted under mandate, and political direction of multinational organizations (UN, EU, NATO, OSCE, etc.), or by a coalition created by voluntary agreements. The typical solution is a group of organizations created a mission-oriented way, and usually with organizational changes in time, the combined joint task force in NATO terms.

Common responsibility of NATO member countries to reach common security goals and to support common security interests is demonstrated by the increase in the amount and decrease in the unit size of multinational organizations. In the 1960s basic building blocks of NATO forces were national corps. After a force restructuring these were succeeded by multinational corps of national divisions, and later by multinational divisions based on national brigades. In our days one can encounter more and more multinational brigades, or even battalions, established bi-, or multilateral agreements. In case of Hungary the examples are the Italian-Slovene-Hungarian brigade, the Hungarian-Romanian battalion, or the Hungarian-Ukrainian emergency response battalion.

Since last decades of the 20th century the forces created to conduct crisis response operation – with some exceptions – have been multinational forces, where different organizations of the same nation, organizations of an alliance, or units of a coalition established to accomplish a mission worked together. In most operations, in addition to military organizations other governmental (e.g., administrative, or police), and non-governmental, or public voluntary organizations are working in the area of operations, with whom military organizations, in order to achieve common, or partially overlapping goals, have to cooperate to a certain extent, or at least to exchange information. This was the case in the first Iraqi war, in the operations on the Balkan, in the crisis management on East Timor, in the intervention in Afghanistan, and last time in the second Iraqi war.

Basics of information interoperability

The fundamental condition of successful and efficient operation of complex organizations, organizational systems, groupings is the sufficient level of information exchange between components, the sharing, and coordinated exploitation of information necessary for cooperation. In case of heterogeneous components there is an additional condition, the information interoperability of the cooperating forces that in our opinion, in its broader sense can be defined in the following way:

> *Information interoperability is a mutual capability of different actors necessary to ensure exchange and common understanding of information needed for their successful cooperation.*

Information interoperability can be interpreted in partly different, but analogue manner in case of individual persons, and organizations. Concepts of information, and knowledge in our interpretation are connected to human mind.* The previous is a reflection, an inner, mental representation of a delimited aspect of the world, and the later is the mental representation of the whole world. In the course of information exchange between people one party (the sender) transforms a piece of his/her knowledge into a representation appropriate for transmission, and this outer representation gets to the other party (the receiver), who interprets it, and develops an own inner, mental representation, and inserts it into his/her knowledge. Thus eventually not the information itself is transmitted, but it is represented, the representation is transmitted, and an "other" information created on the basis of this representation.

Common understanding means, that parties of information exchange perceiving identical items of communication, interpreting identical outer representations develop an appropriately identical mental representation (in this case appropriately identical for the purposes of cooperation). In other words common understanding means that the interpreted meaning of the given representation developed by the receiver corresponds with a required level to the intended meaning, determined by the sender.

In case of information exchange between organizations, organizational information is interpreted – analogously to the concept of personal information – as a reflection, inner mental and/or outer representation of a delimited aspect of the world, in the organization. So organisational information can simultaneously exists in both form, in

* Details can be found in (MUNK, 2002b).

the mind of members of the organization, and in the form of some outer, recorded representation. These later can be recorded on traditional media, and stored in information systems, devices, and applications in “informatical” formats.**

The basic model of inter-organisational information exchange consists of the following tasks:

- some piece of information in the human mind represented in an appropriate representation (if required);
- representation resulted from the previous step, or already existing in recorded format is transformed to an intermediary representation appropriate for transmission (if required);
- intermediary representation is transmitted to the receiver;
- intermediary representation received is transformed (back) to a representation appropriate for the receiver (if required);
- the resulted representation is interpreted, transformed to information, i.e. to an inner mental representation (if required).

As it can be seen from the above, almost all steps of the information exchange process – except for transmission of the intermediary representation – are representational transformations, where the basic requirement of the information interoperability (the information exchange based on common understanding) is to preserve the intended (planned) meaning carried by representations.

Information interoperability and warfare of the information age

At the end of the 20th century a lot of new ideas, and concepts appeared about the warfare of the information age. No doubt that two of these ideas play significant role in research papers in military sciences, in doctrinal documents, and military visions: information superiority, information operations, and network centric warfare. This section will survey the most important relations between these fundamental ideas, and information interoperability.

Information interoperability and information operations

Fundamental concept of information warfare, and information operations is Information Superiority, which – by an explanation appearing in a comprehensive book of a US research group – is “a state of imbalance in one’s favor (relative advantage) in the information domain that is achieved by being able to get the right information to the

** In our days this format is typically, but not exclusively electronic and digital.

right people at the right time in the right form while denying an adversary the ability to do the same.” (ALBERTS et al., 2001)

One can found some other definitions of information superiority that can be used to deduce the fundamental, commonly accepted features of this concept. In our opinion the essence of the concept in the broader sense can be described by the following definition: information superiority is a difference in one's favor (relative advantage) in the information capabilities of the parties affected, and that can be realized in operational – in case of military application in military operational – results. Difference in information capabilities should not be restricted to information processing, and communications capabilities, or to the differences between amounts of information they possess. Moreover information capabilities cannot be measured on an absolute scale, but they should be related to the information requirements.

The four basic possibilities to develop, and maintain information superiority are: to enhance, and optimally utilize own information capabilities; to protect own information capabilities against different threats; to destroy, deny, or affect adversary information capabilities; and at last to influence other actors in the information domain in own interests. From the point of view of interoperability the first category of activities is worth detailed discussing.

Enhancement, and optimal utilization of own information capabilities can be achieved by the following: to acquire, and collect more, and better quality information about the environment, and the relevant actors; to develop a more accurate, valid, and organisation-level (common, shared) situational awareness, based on the collected information; to harmonize, coordinate goals in a more detailed manner; to create more exact, well founded forecasts for a longer timeframe; to determine more justified, commonly understood tasks from the common goals, shared situational awareness, and forecasts; and at last to develop more accurate, coordinated plans for the execution.

Most of the tasks enumerated above require not only individual information processing capabilities of the cooperating actors, organisational components, but exchange, and sharing of information between them. For lack of information sharing a sufficient level of common situational awareness, necessary for efficient cooperation cannot be developed, and maintained, and similarly harmonization of goals, appropriate knowledge of tasks, and coordination of plans cannot be ensured. All these require information interoperability between cooperating actors.

Information interoperability and network centric warfare

Network Centric Warfare (NCW) is the most frequently used, and most appropriate expression so far for a conceptual description of the forces, and operations of the

Information Age. By a definition of distinguished experts of this topic, network centric warfare is “an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of selfsynchronization. In essence, NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace.” (ALBERTS et al. 1999).

The main features of a network centric force are the following: geographically dispersed; knowledgeable (with advanced information capabilities), and effectively linked (networked). As a consequence of technological progress, development of communication, mobility, and execution capabilities, combat power has been increasingly freed from the location of battlefield components, assets. Components with advanced information capabilities, having a shared, common knowledge of the situation and commanders’ intent are able to self-synchronize, operate with a smaller footprint, and be more effective when operating autonomously. Fundamental condition of effective linking is a robust, high-performance information infrastructure, or infostructure.

Linking, networking of the force – a prerequisite to be network-centric attribute – should be done in three domains. In the physical (material) domain all elements of the force should be securely, and seamlessly connected into a robust network. In the information domain the capability to organisational level collection, sharing, access, and protection of information, and information level collaboration (correlation, fusion, analysis) should be ensured. And at last in the cognitive domain development, and maintenance of a suitable level of shared situational awareness, and shared knowledge of commanders’ intent should be ensured.

Principles and solutions of network centric warfare follow the previous, platform centric solutions. Previously information gathering (sensor), decision (command and control), and execution (shooter) functions, and the appropriate system components usually were integrated into one equipment system, were implemented on one platform, and their information links existed mainly with each other. Whereas the network centric warfare characterized by the increased autonomy, in many cases even physical separation of functional components, and the increase of their interconnections. During execution the network centric force operates as a virtual organization built from appropriate components, linked by information connections.

As a consequence of the above network centric force is characterized by an increased, dynamically changing system of information connections. Components to mutually exploit, and strengthen each others capabilities, to attain synergetic effects have to be able to exchange information with organizations with both similar, and both different functionalities (this naturally does not mean that information exchange have to be ensured between any two component). This exchange of information obviously should be realized in a manner based on common understanding, so information interoperability should exist between components of a network centric force.

The role, and importance of information, and semantic interoperability in network centric warfare was emphasized in a report of the Department of Defense of the United States to the Congress as follows: "Network Centric Warfare is based upon the ability of a force to develop shared situational awareness in the cognitive domain. Technical interoperability will get us to the point where the information is correctly represented in distributed systems, but does not ensure that the individuals in different locations, in different organizations, at different echelons have a similar understanding even though they 'see' the same thing. With the added complexity of coalition operations that involve different cultures, the problem is greatly compounded. Semantic interoperability is the capability to routinely translate the same information into the same understanding. This is, of course, necessary to develop the shared situational awareness upon which mature forms of Network Centric Warfare are based." (*DoD Report*, 2001).

So it can be summarized that without information interoperability there is no network centric force, there are not possible network centric operations. Linking to information infrastructure, and information exchange with other components require all three levels of information interoperability. Dynamically changing connections between components highlight in particular the importance of semantic interoperability, because in this new environment the components have to be able to efficiently exchange information with much more and different partners.

Concept and significance of semantic interoperability

The fundamental concept of semantics is meaning assigned to environmental effects, messages, and data during information acquisition by, and information exchange between humans. In the course of sensual cognition, and communication human beings first perceive, sense, then interpret these effects, messages, and data, and at last build them into their knowledge. Concept of information is strongly connected to meaning that is illustrated by the following expressions: "meaning assigned to data by means of known conventions", "data in context as understood by an individual" (*ADatP-32*, 2001).

In this sense meaning, and in consequence information is subjective, strongly connected to individuals. It is because reflection of the same environmental effects, messages, and data is usually different in different people depending on their goals, motivations, and actual knowledge. Identical (if it is possible at all), or similar reflection can be reached only in the course of cooperation, or with communication. Common interpretation, developed and confirmed in practice, is a prerequisite of successful cooperation, and communication.

Concepts used with common understanding in a group of people, and information based on these concepts is no longer dependent on subjectum of individual members of the group. All members of the group perceive, and interpret the environmental effects, things and phenomena of the world in the same way (to be more precise, as we have said earlier: in a way similar enough for cooperation), so they can also provide and receive information about these objects with (sufficiently) identical content and meaning. These concepts, and information are group-subjective (or inter-subjective), because they depend on the common, agreed interpretation of the group. In this sense we can talk about the meaning of an environmental effect, message, or data, pertaining to a given group.

Concept and interpretation of semantic heterogeneity

With the widening of cooperation, and with the broadening possibilities of information exchange, more often happens, that there do not exist the conditions of sufficient common understanding between cooperating parties. The most suitable to characterize this situation is the concept of semantic heterogeneity that rather rarely appears in literature but we can find the following definition in a publication:

> "Semantic heterogeneity … occurs when there is a disagreement regarding the interpretation and intended use of related information, or when the same phenomenon in a Universe of Discourse is modelled in different ways in two systems." (JOHANESSON-JAMIL, 1994)

This definition includes components connected both to people, and to (technical) systems, that in order to get a more precise interpretation we should examine separately.

In case of people – although the expression in this context is rarely used – semantic heterogeneity means lack, or an insufficient level of common, shared interpretation (understanding). In restricted sense this pertains only to direct, or indirect information exchange between people (messages, and data), but in broader sense it also extends to the interpretation of environmental effects.

For the purposes of storage and transmission, or operation of automated devices, different components of human knowledge can be recorded, stored, and utilized using traditional or electronic media, or systems. Knowledge components objectified in different forms (text, data, program, rules, drawing, picture, audio, video, etc. and any combinations of these) usually are available for other people to use. Information storage, and processing devices obviously are not able to interpret data stored, or processed, they ‘do not know’ their meaning. Only people utilizing these devices can assign meaning to data.

So only an intended meaning, planned interpretation can be assigned to knowledge components stored on information media, or in information systems (and any devices with information functions), and it should be connected to users of these systems (devices), or to information providers. The intended meaning, agreed intentions, and interpretation of the primary users are usually determined in the purpose and functional requirements of the given system. Conditions of common interpretation suitable to purpose of the given system can be ensured partly by direct communication with primary users, partly by different documentations supporting application of the given system.

So we interpret semantic heterogeneity between people and technical systems as a difference between the interpretation of a given user, and the common interpretation of the primary users about data stored in, or functions provided by the given system. Semantic interoperability between technical systems can be interpreted in the same way. In this case heterogeneity is the difference between intended meanings of knowledge components stored in the two systems that is between common interpretations of the two groups of primary users. This is expressed in the following definition.

> *Semantic heterogeneity is a disagreement regarding the interpretation of identical things (environmental effects, messages, data). In case of technical systems interpretation means intended meaning, agreed by the group of primary users.*

Concept and interpretation of semantic interoperability

According to an interpretation (see detail in MUNK, 2002a) interoperability is a mutual capability of different objects to ensure successful and efficient cooperation. So concept of interoperability really has sense only in those situations that characterized by some forms of heterogeneity. So semantic interoperability can be also interpreted in connection with semantic heterogeneity. The publication referenced earlier describes this as “cooperation among semantically heterogeneous systems” (Johanesson-Jamil, 1994).

The referenced explication is in conflict with some basic components of the concept of interoperability. On the one hand it does not define the concept as a mutual capability, but emphasizes the existence of cooperation. On the other hand it does not say anything about the quality of cooperation. So the following definition with a more general meaning should be useful:

> *Semantic interoperability is a mutual capability of different actors to exchange representations of information necessary for efficient cooperation, in a way that preserves meaning (with transformations if required).*

Similarly to semantic heterogeneity, semantic interoperability can be interpreted, and examined between people, between people and technical systems, and between technical systems. In the age of the IT revolution, the most important, but at the same time the most difficult is the third of them: semantic interoperability between IT systems, devices, and applications. Up to the mid of the 1990s the research in this area was mainly concentrated on resolving heterogeneity of different databases, database schemas. At the end of the 20th century, based on results in artificial intelligence, research on formal description of conceptualisation was becoming increasingly widespread, because it proved to be necessary to develop and implement explicit descriptions of semantics (e.g. ontologies) for IT systems.

It is obvious that as operational interoperability plays primary role regarding interoperability in general, semantic interoperability plays primary role regarding information interoperability. To ensure purposeful interoperability between IT systems, and applications, and efficient use of heterogeneous infosphere elements it is necessary to study problems of semantic heterogeneity, methods and tools ensuring semantic interoperability on every field of practice, so in military area too.

Summary

Successful execution of different – military, disaster relief, humanitarian assistance, etc. – operations of our age requires strong cooperation of the participating actors (organizations, persons) with different capabilities, and coordination of their activities. Fundamental condition of successful and efficient cooperation is the sufficient level of information exchange between components, the sharing, and coordinated exploitation of information necessary for cooperation. Military forces are heterogeneous in many different areas, so information interoperability is a prerequisite of successful information exchange. Heterogeneity appears in the differences based on the division of labour, field specialization; in technical systems, and equipments; and the procedures, and methods applied. In our days, in consequence of increasing importance of multinational operations, degree and role of these types of heterogeneity have essentially grown.

Information interoperability is a mutual capability of different actors necessary to ensure exchange and common understanding of information needed for their successful cooperation, that has a basic requirement: to preserve the intended (planned) meaning carried by information representations used in information exchange. Some emerging concepts of the information age warfare (information superiority, network centric warfare) are in strong connection with information interoperability. One of the basic possibilities to develop, and maintain information superiority is to enhance own information capabilities, the capabilities of information sharing, and shared understanding. A network centric force is characterized by an increased, dynamically changing system of information connections. Components to mutually exploit, and strengthen each others capabilities have to be able to exchange information with organizations with both similar, and both different functionalities.

Information interoperability can be divided into three levels: the physical (material) level of mediums used; the syntactical level of languages, message- and data formats; and the semantic level of content, and meaning to exchange. In our days interoperability on the two first levels can be realized relatively easily. Much more difficult to ensure the common interpretation (semantic interoperability) of data transmitted in messages, stored in, or accessed from databases, and functions, services provided by information systems. This has importance in case of semantic heterogeneity, that is a disagreement regarding the interpretation of identical things. The concept can be interpreted between people and technical systems, and betweem technical systems, based on the intended (planned) meaning. Semantic interoperability interoperability is a mutual capability of different actors to exchange representations of information necessary for efficient cooperation, in a way that preserves meaning. Implementation of semantic interoperability is a significant condition of the successful warfare in the information age, so further researches in this field are important for military sciences.

References

ADatP-32, (2001) Part I, The NATO Corporate Data Model. Concept and Description. NATO HQ C3 Staff, NATO Data Administration Office, Brussels.

ALBERTS, D. S., GARSTKA, J. J., HAYES, R. E., SIGNORI, D. A. (2001): *Understanding Information Age Warfare.* CCRP Press, Washington.

ALBERTS, D. S., GARSTKA, J. J., STEIN, F. P. (1999): *Network Centric Warfare. Developing and Leveraging Information Superiority.* 2nd Edition (Revised) CCRP Press, Washington.

DRIESENAAR, F. N. (2001): Information exchange in support of C2-Interoperability. In: *RTO Meeting Proceedings 49. New Information Processing Techniques for Military Systems.* NATO Research and Technology Organization, Neuilly-sur-Seine. (pp. 1-1–1-8).

JOHANNESSON, P., JAMIL, M. H. (1994): Semantic interoperability. Context, issues, and research directions. In: BRODIE, M. L., JARKE, M., PAPAZOGLOU, M. P. (Eds): *Proceedings of the Second International Conference on Cooperative Information Systems, May 17–20.* Toronto (pp. 180–191).

MUNK, S. (2002a): An analysis of basic interoperability reletad terms, system of interoperability types. *Academic and Applied Research in Military Science*, 2002/1: 117–132.

MUNK, S. (2002b): Információs színtér, információs környezet, információs infrastruktúra. *Nemzetvédelmi Egyetemi Közlemények*, 2002/2: 133–154.

Network Centric Warfare. Department of Defense Report to Congress. (2001) Department of Defense USA.