AARMS
Vol. 5, No. 1 (2006) 105–114

Some consequences of the network centric approach

SÁNDOR MUNK

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

Network oriented approaches are emerging components of our days' military visions. These approaches are strongly connected with, and based on information exchange between/among cooperating elements of a networked force. All network centric concepts share the same simple, yet powerful idea – that information sharing is a source of potential value. In this paper we summarize the basics of the network centric approach from the point of view of information sharing, analyze the consequences and requirements of the network centric approach to the cooperation environment, and finally discuss the role of information interoperability, different solutions (levels) of "network centricity" and give reasons for the necessity of an interoperability infrastructure in a network oriented environment.

Introduction

The long term vision of the two NATO Strategic Commanders[1] highlights, that "Future military forces must be … capable of operating in a networked environment. These forces must be rapidly tailorable and fully interoperable with other military forces and capable of interacting seamlessly with civil authorities, non-governmental organisations and other agencies in the joint operations area." It also states, that "The capabilities required to be successful in the future environment … include: improving intelligence and information sharing …, developing network-enabled capabilities based on a robust and flexible foundation."

NATO Network Enabled Capability is one of the network oriented approaches, that is still under development within NATO and its member nations. NNEC supports a new mode of military operations which heavily relies upon information-based and network-based capabilities and strategies. Network oriented approaches are strongly connected with, and based on information exchange between/among cooperating elements of a networked force. All network centric concepts share the same simple, yet powerful idea – that information sharing is a source of potential value.

Network centric operations are based upon the ability of a force to develop a shared situational awareness in the cognitive domain. A truly networked force includes different and dynamically changing components, so one of the main tasks of realization

Received: January 10, 2006

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

of any network centric approach is to ensure information interoperability (including semantic interoperability). This paper summarizes fundamental concepts and characteristics of network centric approaches, analyses consequences of network centric approach, presents its links to information interoperability, and finally discusses different solutions (levels) of "network centricity".

Basics of the network centric approach

Network centric approaches support a new mode of military operations which heavily rely upon information-based and network-based capabilities and strategies. Different network centric concepts are the most frequently used, and most appropriate expressions so far for a conceptual description of the forces, and operations of the Information Age. The first concept was network centric warfare (NCW), that - by a definition of distinguished experts of this topic – 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 self-synchronization. In essence, NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace."[2]

Accross NATO member nations various network centric initiatives are denoted by different terms, e.g. Network Enabled Capability (NEC), Network Based Defence (NBD), Network Based Operations (NBO), Network Centric Warfare (NCW), and Network Centric Operations (NCO). The NATO Network Enabled Capabilities (NNEC) strives to integrate different national approaches, and products. The current working definition states, that "The NATO Network Enabled Capabilities (NNEC) encompasses the elements involved in linking collectors, effectors and decision-makers together to enable the development of a NATO, network-centric, effects-based, operational capability. This will involve the Joint Deployment and Sustainment of forces, that are able to translate information into increased combat power and mission effectiveness through Decision Superiority, leading to rapid, flexible, precise, coherent operational effects."[3]

According to the US approach, 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.

The NATO view was formulated in a conference, organized by Headquarters Supreme Allied Command Transformation in March 2004. It was commonly accepted, that network centric approach is more about people, and organizations to work together in new, more dynamic, flexible and effective ways than it is about technology. Yet it is technology that provides information with the scope, speed, and richness necessary to enable this transformation to take place. The four fundamental NNEC concepts are: robustly networked force, information sharing, dynamics and flexibility, and inclusive and flexible acquisition.

A robustly networked force is one of the key prerequisites for NEC. The NEC environment is intended to provide seamless end-to-end capabilities to all war fighting, national security, and support users. It will consist of national, allied, and coalition network infrastructures comprised of all types of communication networks including strategic high-speed networks, tactical ad-hoc radio networks, and wireless networks supporting transmission of data, voice, and video. The goals of this network enabled environment are protected, assured, interoperable communications. In addition, the information infrastructure must be resilient to ensure information is managed coherently across the NEC environment.

Information sharing of all sources of information that are relevant to the mission is a highly complex issue, since the NEC environment will include of many different assets of many different nations. The level of information sharing, affected among others by security interests of participants, has a direct impact on the closeness, ease, and efficiency of the collaboration possible. The NEC environment also requires a high degree of dynamics and flexibility, it encompasses the dynamic creation and authorized reconfiguration of assets to meet the mission needs.

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.

Consequences of the network centric approach

In a simplified way, a network centric force can be characterized by the famous goals of French revolution: liberty, egality, and fraternity. At first, elements of a networked force freely build and realize their capabilities, freely share these with other elements, and take part in collaboration in their own interests. Secondly elements autonomously take part in the cooperation, their interconnections, and links based on their equality, not on a strict subordination. And lastly elements cooperate to reach commonly accepted, harmonized goals, in a fraternal way.

An important consequence of network centric approaches is the increased heterogeneity of participants, and assets of a network centric force. 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. The next version of heterogeneity appears in the differences in technical systems, and equipments of organizations, organizational elements with same functions. Heterogeneity in equipments is mostly natural, and mostly unavoidable. 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 outer environment (doctrines, directives, regulations, etc.), the personal qualities and attitudes of the members of the organization, and the organizational traditions, cultures.

Warfare of our age (and especially the emerging network centric warfare) is based on a dramatically changing system of information links. So components of the armies (organizations, persons, and technical, mainly information systems), need to have new types of capabilities. Necessity of information exchange between forces conducting military operations is not a new requirement, because successful and efficient realization of operations, composed of organized, coordinated actions was always, and is impossible without exchange of information. Novelty, fundamental feature of

network centric approaches is in the characteristics of the battlefield entities, in the structure of their "network", in the quantity of their interrelationships, and in the amount and nature of information flowing among them.

Information exchange networks in "traditional" armies – among others due to the limitations of the available communication systems' capabilities – are characterized by relatively small number of links, that in accordance with the chain of command, are mainly hierarchical, and are complemented by horizontal links (between neighbors, and supporting-supported organizations). In contrast with this, a network centric force is characterized by an enhanced, mission-, and situation-oriented, dynamically changing system of information links.

To achieve synergistic effects, to mutually exploit each other's capabilities, force components should be able to seamlessly exchange information with other components of similar, or dissimilar functionality (this doesn't mean, that information exchange should be made possible between any two components). It is obvious, that information exchange should support efficient operation, and should be based on common understanding, so in other words, it is necessary to create, and maintain information interoperability between components of a network centric force.

Successful operation of individual battlefield entities more and more depends on information coming from other entities, and they are, to a greater extent, sources of information for other entities. Cooperation with other components not belonging to a given parent organization continually extends to more and more lower organizational levels, even in some cases to individual systems, and devices. So information interoperability, and information security questions, and problems should be examined, and solved in increasingly lower levels.

Role, and significance of information, and especially semantic interoperability from the point of view of network centric warfare has been worth mentioning in a report of the Department of Defense to the Congress of the United States of America: "Network Centric Warfare is based upon the ability of a force to develop a 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."[4]

As a consequence, it should be pointed out, that there is no network centric force, there are no network centric operations without information interoperability. Connectivity to information infrastructure, and information exchange with other entities requires implementation of all the three levels of information interoperability. Dynamically changing links between entities highlight the role of semantic interoperability, because in the new, information-rich environment entities should be able to exchange information efficiently, and seamlessly with much more, and different entities, than before.

Network centric approach and information interoperability

Different assets, platforms, systems, or organizations should have appropriate capabilities to work, and cooperate in a network centric environment, as a component of a network centric force. The UK concept of Network Enabled Capability formulates the following definitions. A system is 'net ready', if it "can be configured to make immediate use of the supporting information infrastructure and services, and work seamlessly with other assets, regardless of the location or without requiring dedicated infrastructure information services". A platform is 'network ready', if it is "equipped and configured to exploit network services in order to provide the information necessary for other platforms to deliver their full potential or to use the information obtained by others to deliver their own."[5]

It is almost obvious, that a system, or platfom cannot easily be made interoperable with any other element of a network centric force, and with the continually growing, and extending infrastructure services. Depending on the realization of information interoperability, the characteristics of the information exchange between cooperating actors, and the supporting information infrastructure, "network centricity" can be implemented in three levels. The simplest level is the elementary model, that is a networked capability between/among elements who belong to the same functional area, or specialization, and who are in a relatively strong and permanent cooperation. The next level is the complex model, that is also connected with a relatively permanent cooperation, but it covers more, or all possible functional (cooperation) areas of an organization. And finally the highest level is the global model, where "network centricity" is not restricted to a given cooperation, it describes structures, and solutions in a dynamically changing cooperation and information environment.

In the *elementary model* the strong functional area cooperation usually makes possible to negotiate a preliminary agreement, and if required, to make negotiated changes, modifications on the scope of information to be exchanged, and the

intermediary representation used. So it is possible to define a common intermediary representation ("common language") that is appropriate to exchange of all essential information necessary for efficient cooperation in th networked environment. In this model the transformation between inner representations, and the agreed intermediary representation is responsibility of the elements themselves. This ensures the autonomy of the elements, and makes easy to extend the cooperation.

Elementary "network centricity" is the basic, and minimally necessary solution to resolve heterogeneities between cooperating partners, but its extensive implementation has serious limitations. One of the problems is that a preliminary agreement on an intermediary representation is always connected to a given group of cooperating actors, and even on the same, or similar functional areas there can be more, or several agreements, different intermediary representations. Because of the essential sameness of the functional area, these representations usually differ only in format, not in the concepts used.

Despite of standardization efforts on several application areas (e.g. engineering, public health, bibliography, or meteorology) there are different interoperability solutions, exchange languages, formats. In military application, examples of parallel solutions are the exchange formats used on the same functional area, but in different military forces (e.g. USMTF, ADatP-3), or in different armed services of the same military force (USMTF, OTHT-GOLD), and the different versions of tactical data links with similar, or identical purpose (e.g. Link-1, Link-11, Link-16, and Link-22).

The *complex model* is connected with complete organizations, and organizational systems, and characterized by more intermediary representations. In this model the different representations form a harmonized system, all of them have special role – to support definite elements, and a definite part of the complex information exchange. In a broad cooperation environment elementary representations, used on basic functional areas, usually significantly overlap each other. So to support information exchange between different functional areas, higher level intermediary representations are needed to resolve heterogeneities between elementary intermediary representations. In a complex cooperation environment this requires a multilevel, usually hierarchical system of representations.

In practice only elementary interoperability solutions for individual functional areas appeared so far. Even the theoretical analysis of the complex interoperability model has just begun. One of the most elaborated discussions can be found in a paper of Lasschuyt,[6] who analyses interoperability questions based on multiple intermediary representations from the point of view of a highly complex cooperation environment, the NATO C3 systems. Elementary, and complex level solutions can be used to

implement a national level network enabled capability, but they are inadequate in a multinational, allied, and coalition environment.

The *global model* uses a fundamentally different approach. While the previous two models were based on a group-, and organization-oriented approach, this third model describes the interoperability problems, and solutions from the point of view of individual actors in the infosphere. In our days an actor has to cooperate with a lot of such other actors with whom there is no real possibility to preliminarily agree on the information to be exchanged, and its representation, and whose conceptual systems, and native representations are significantly different.

In such a situation it is necessary, that a given system should be capable in a dynamically changing way, and in relatively short time to exchange information using previously unknown representations. This dynamic interoperability capability obviously can not be absolute, but within some limits it can be realized. Since the number of representations on the syntactical level is relatively small, and grows slowly, a capability of transformations between the possible representations on this level can be implemented in advance. As a consequence of individual conceptual systems, and points of views the harder task is to realize semantic level transformations, that is actually not a development-oriented task requiring first of all (software) technical knowledge, but an application-oriented task requiring mostly domain knowledge.

Ensuring dynamic interoperability necessary for actors of the global model can not be efficiently implemented as part of the affected systems (platforms), since it would require continuous modification, development of this systems, but not in their basic parts. So the required transformation functionalities should be realized in form of independent infrastructure components, built especially for this purpose. This leads to the concept, and questions of information interoperability infrastructure.

Information interoperability infrastructure is a coherent system of methods, means, and services, that's purpose is to support information exchange between cooperating actors in a meaning preserving way. Two fundamental tasks of this infrastructure are transformations between different information representations, and transmission of intermediary representations between actors during information exchange.

Transformations between inner, and intermediary representations today usually implemented as an integrated part of a given system, or platform. So when a new intermediary representation appears, a new interface application component needs to be developed for every system. The main disadvantage of this approach is that the same, or very similar functionality need to be implemented more or less independently, in a hidden, not reusable way in many versions. The main role of every infrastructure is to collect, implement, and provide every usable function, or service for a wide user

community. In practice every infrastructure was born from individual solutions: separated from existing systems; redesigned, generalized, and reimplemented in a unified, centralized manner.

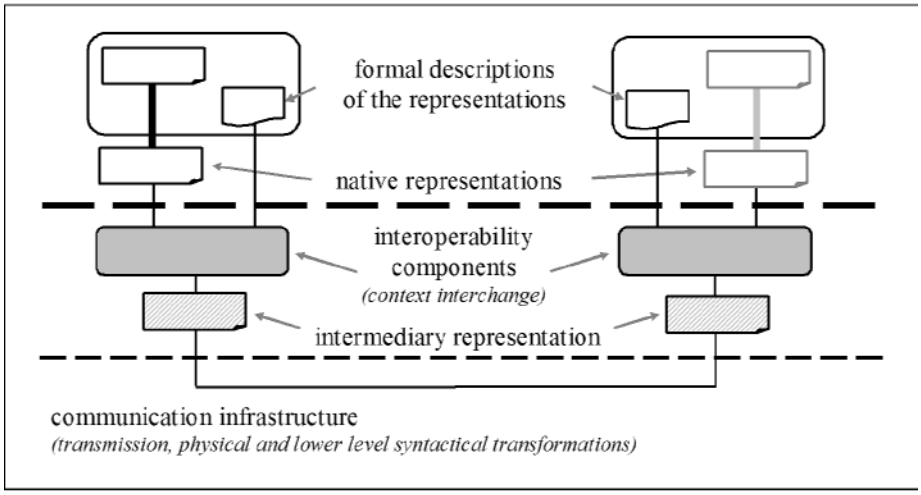

Figure 1. Interoperability infrastructure

An information interoperability infrastructure should be implemented as a complex network of different components with well-defined functions. This is not only because we live in an increasingly network-oriented, network centric world, but also because almost any traditional infrastructure is, and was essentially a network of service-provider, and communication components.

Summary, conclusions

Emerging network centric approach, appearing in society, economy, and warfare of our age does not only creates information interoperability requirements, not only increases the role, and significance of information interoperability, but suggests a new way to its implementation. Traditional ways of ensuring information interoperability of heterogeneous systems, as elements of a networked force seem not to be appropriate.

In a dynamically changing information environment the adaptation based on a continuous development neither sufficiently efficient, nor flexible, and in some cases even can not be accomplished. Even a minor system upgrade, limited in range and

volume, requires a significant amount of time from the formulation of the requirements to the implementation of the new software or hardware version (solution). Moreover an additional time is necessary to do the modifications on all of the working implementations of the given system. What is more, in case of "legacy" systems usually it is not possible to upgrade the system, to extend it with a new interface functionality.

Network centric approach – that is, among others, characterized by the improved accessibility, autonomy, even detachment of different capabilities, and functions earlier strongly connected to, or inherently built into a "platform" – can be used in case of application components ensuring information interoperability, supporting information exchange among heterogeneous cooperating information systems. The result should be an information interoperability infrastructure, that is an inherent part of the information infrastructure of a network centric environment.

Although some professionals say that we don't need deal with "high-tech" questions, and problems, appropriate scientific research and development activities should be done in this field in the Hungarian Home Defense Forces too. Hungarian military units (contingents) take part in different NATO, EU, and coalition operations, and they will soon "work" in a continuously "networked" environment. Enabling successful and efficient operation in a partly unforeseen and dynamically changing cooperation environment, these formations will need an appropriate information (and IT) interoperability solution.

References

1. *Strategic Vision: The Military Challenge. By NATO's Strategic Commanders*. Allied Command Transformation – Allied Command Operations, 2004.
2. ALBERTS, D. S., GARSTKA, J. J., STEIN, F. P.: *Network Centric Warfare. Developing and Leveraging Information Superiority.* (2nd Edition). CCRP Publication Series, 2000.
3. *NATO Network Enabled Capabilities (NNEC) definition.* – NATO ACT website (July 2004).
5. *Network Enabled Capability Outline of Concepts*. Issue 2.0. Part 1-10. (2003) DSTL – IMD – SOS.
6. LASSCHUYT, E.: *Information Interoperability Domains.* NATO Research and Technology Organization, 2003.