

Challenges of Implementation of the Network Centric Warfare Tenets in Coalition Environment

*By Arturas Litvaitis**

Contemporary global security challenges dictate the necessity for timely and efficient response. Today the United States is perhaps the only nation able to independently conduct wide-scale military operations in any place around the world. However, gradually increasing number of hotspots makes the burden too heavy even for this superpower. Taking into account not only military capabilities but also probably an even more important need for a broad international support for the United States, it is evident that, today and most likely in the future, the United States would need to act in the coalitions with the traditional allies (AUSCANNZUKUS, NATO, EU) as well as other nations willing to join U.S.-led operations. Despite the fact that NATO takes over some responsibilities in the role of security provider beyond the Euro-Atlantic region (for instance, the International Security Assistance Forces in Afghanistan), the United States still remains a key player shaping military operations now and in the future.

Since the last decade of the 20th Century, the United States have launched a number of initiatives of its armed forces transformation with the purpose to more effectively meet the modern security challenges. One of the key elements of the U.S. defence transformation is Network Centric Warfare (NCW) – a concept of military response to global evolutionary transition from the Industrial to the Information Age (Office of Force Transformation, 2005:3-6). First time officially introduced¹ in the Department's of Defence Report to Congress (Department of Defence, 2001:4-1), Network Centric Warfare is a concept of modern warfare bringing all elements of forces – shooters, sensors, decision makers etc. – to a unique by its nature integrated network, supposedly providing an increased battlespace awareness and, as a result, a competitive advantage over an adversary via faster and more precise decisions and actions.

* Major Arturas Litvaitis, Lithuanian Armed Forces, is a graduate of the Joint Command and General Staff Course 2007/2008 of the Baltic Defence College. The article is based on his Individual Study Paper, therefore the thoughts and views expressed in this article are those of the author and do not represent the official position of the Lithuanian Armed Forces.

The tenets of NCW set the stage for further theoretical and practical developments not only in the United States, but also served the purpose of being a point of departure for other nations' research and development. Besides the individual nations, NATO started to develop its own concept, NATO Network Enabled Capability (NNEC), which also had started from the tenets of NCW (NC3A, 2005:3). Therefore the tenets have their impact for the entire North Atlantic community, today comprising 26 nations with their, however, uneven attitudes towards the network-centric concepts.

I would argue that implementation of the NCW tenets in a multinational environment would not take place in the near future, if at all, in their current formulation, because human's intention and will to work together, despite of being the driving factors, are not obvious in all cases. I cannot overcome the feeling that the proponents of NCW were not so much concerned about the potential challenges of concept's implementation in the multinational environment, so it seems that they were drafting the concept exclusively for the U.S. use. To be honest, multinationality is mentioned in some books and documents about NCW; however, it doesn't seem that the developments over the last decades in the area of alignment of different nations' military capabilities took into account very carefully the need for procedural, operational and technological interoperability. Finally, I think that probably the most important issue is often forgotten in the NCW concept – diversity of human beings in all possible dimensions, such as culture, language, and perceptions. The state-of-the-art hardware and weaponry will not bring any good if not animated by human intellect, will and creativity; therefore not steel, semiconductors or lasers are precluding the greater success of military operations – usually the biggest obstacle is somewhere inside of our brains.

Bearing in mind these remarks, I would like to suggest taking a look at some issues that the United States and its allies could face when implementing the Network Centric Warfare concept in the future coalitions. However, this article does not have ambitions to cover all possible issues of implementation of NCW in the coalition environment, nor to provide an in-depth analysis. Rather, the intent of this article is to possibly inspire further discussions and research.

Trying to answer the question of what could be the possible challenges of NCW implementation in the multinational coalition environment, in this

article I, firstly, will provide a general review of main ideas of the NCW concept as presented by its promoters, and then turn to the critical views on the concept. Later, I will analyze, in my opinion, key problematic areas of building coalition communications networks. In the first part of the last section I present my analysis of how a dynamic multinational environment may affect military teams' capability to build common knowledge, whereas in the second part of the last section I will focus on the possible influence of cultural diversity on general perception of Network Centric Warfare and its major notions such as sharing of information, self-synchronization and others.

1. Setting the stage

According to the proponents of Network Centric Warfare, the need to shift the approach of conducting military operations is determined by radical changes in the society, where implementation of modern technologies transformed the ways of wealth creation and distribution of power as well as increased complexity, reduced distances and increased pace of everyone's life (Alberts, Garstka, Stein, 1999:15). The analysis of business processes shows that information itself is becoming a significant value and source of power nowadays, therefore the extensive exploitation of information is a prerequisite to be successful on the market (Ibid:29-51). Assuming that the same or similar laws are applicable to the military world, those trends were applied by military theorists and translated into the concept known as Network Centric Warfare. Setting the stage for further analysis, in this section I suggest, first, to overview the basic constructs of the Network Centric Warfare, and later, in order to have a more complete picture of the issue, I will present some critical views on this concept.

1.1 Network Centric Warfare concept

Network Centric Warfare concept, in some sources called as an "emerging theory of war in the Information Age" (Office of Force Transformation, 2005:3) could be shortly presented by (and actually is based on) four tenets (Department of Defence, 2001:4-1):

1. A robustly networked force improves information sharing;
2. Information sharing enhances the quality of information and shared situational awareness;

3. Shared situational awareness enables collaboration and self-synchronization, and enhances sustainability and speed of command;
4. These, in turn, dramatically increase mission effectiveness.

It is easy to notice that each later tenet is resulting from the former; therefore, in fact, we have a chain of resulting principles, instead of a widely used in the military world conceptual approach of “building pillars”.

Let us take a closer look at the meaning of some key terms, used in the tenets' statements. Robustly networked force consists of ready-to-connect (“plug and play”) specialized elements, able to be suppliers of information to the network as well as use the information from other elements of a networked force. In NCW, a strong emphasis is put on the interaction between elements in “peer-to-peer” (horizontal) dimension rather than in traditionally hierarchical (vertical) one (Alberts et. al, 2001:295). Robustness of force networking is a function of ability to maintain network effectiveness despite different conditions and circumstances. Information is fusion of data when latter is put into a meaningful context. Respectively, the quality of information is determined by information completeness, faithful representation of reality (correctness), currency (timeliness), accuracy (level of precision) and consistency for use by other networked force entities (Ibid:82). In each particular instance, requirements for information quality may vary, but information should always be relevant. Shared awareness is the ability of different entities to develop similar awareness of the situation, where degree of similarity is dictated by the level of interactions (working for a common purpose) between those entities; however, in human systems, situational awareness is influenced by culture, language and perceptions (Ibid:26-27). Self-synchronization is the ability of elements of networked force to conduct and synchronize military activities from the bottom up. The prerequisites of self-synchronization are high degree of shared awareness, unity of effort, a clear commander's intent and a common set of rules (Alberts, Papp ed., 2001:486-487). The speed of command is the process of turning informational advantage into faster and more effective military decisions and precise actions, and is characterized by a high rate of change of the initial operational conditions towards locking in own success and locking out the adversary's freedom of actions.

For a better grasp of the environment where NCW takes place, this environment is decomposed into four domains of warfare (or domains of conflict) (Office of Force Transformation, 2004:23-24), sometimes also referred to as the Network Centric Operations (NCO) domains. The first three of those are: physical (sea, land, air and space environments of military operations, platforms, networks), information (where information is created and manipulated - "cyberspace" of military operations), cognitive (perceptions, beliefs, leadership, doctrines by individuals). The fourth one – social domain – was added later, when it was understood that individuals have distinct perceptions of certain phenomena or information and how these individual perceptions play out in case of interactions (e.g. collaborative decision making) within human enterprises, sometimes comprised of participants with quite significant social differences (nationality, language, culture, education, affiliation with certain organizations etc.). As defined by the Network Centric Operations Conceptual Framework, the key elements of the physical domain are the network and net-ready nodes; information domain – data and information; cognitive domain – sensemaking, including awareness, understanding, decisions; and social domain – individual people, practices, including interactions between people, social structures and cultures (Office of Force Transformation, 2004:25-54). I would like to stress that different authors do not always recognize the same main elements of each domain, as well as definitions of domains vary, therefore we have to admit that the Network Centric Warfare concept is not yet supported by unambiguous definitions, which usually causes various interpretations. It also should be understood that warfare takes place in all domains simultaneously and networking takes place within each domain and among them, therefore domains are not isolated from each other, but rather overlapping. Actions or effects in one domain accordingly influence others, thus, taking into account certain ambiguity concerning their elements, the clear boundaries of domains in most cases could not be drawn.

Networked force consists of a number of its elements operating in the domains of warfare, which are called battlespace entities. These are divided into sensors, actors and decision makers. Sensors are the elements providing initial information (data), further processing of which makes the basis for situation awareness. Sensors could be unmanned platforms and equipment as well as human "eyes on the ground". Actors, sometimes called effectors or shooters (Department of Defence, 2005:B-3), are

creating combat power and effects, derived from mission intent and shared situational awareness. Decision makers are people generating mission intent, allocating and re-allocating resources necessary to achieve the desired effects and successfully accomplish the mission. Decision makers are present on all levels of military organization (enterprise).

There are several major conceptual shifts distinguishing the Network Centric Warfare concept from the current way of doing military business. First, it suggests to get rid of current heavy, integrated and thus expensive warfighting platforms, usually comprised of all three elements of battlespace entities. Separation of sensors, actors and decision makers is supposed to contribute to more dispersed, agile and less heavy force, able to achieve greater effects and introduction of less costly specialized platforms and sensors with greater reach and precision. Second, the desired effects are supposed to be achieved by massing the effects rather than by massing the force. Robust dynamic connectivity of the battlespace entities, sharing the information between them will support overall shared situational awareness, which in turn facilitates informational advantage over adversary, more fast and accurate decisions, dynamic allocation of resources and more precise effects. Third, current hierarchical military organizations and corresponding information flows and command and control processes should evolve to more flattened organizations, increasing the information exchange between different levels and services, collaborative planning amongst geographically dispersed entities and capability to make decisions and synchronize actions on lowest possible tactical level. Thus, initiative of actions will come from bottom up rather than from top down as it is in the current military organizations. Summarizing this short overview of the NCW concept, I would like to stress that implementation of this concept will require significant changes in technology, much greater integration of information flow between battlespace entities and new forms of military organizations as well as new forms of command and control.

1.2 The criticism of the Network Centric Warfare concept

The picture of NCW, as a comparatively new concept, could not be complete without an alternative look at it. To complete the picture, here I propose a synopsis of some alternative opinions on the concept and its implementation. At the beginning, I would like to suggest the views of

Ralph E. Giffin (Canada) and Darryn J. Reid (Australia) on NCW. First of all, these authors maintain that the NCW thesis is built on the not necessarily relevant to the military world business analogy in general, and on the discredited nowadays New Economy theory (Lohr, 2001) of fundamental business transformation, influenced by technological progress, in particular. Taking an example of “misinterpretation” of Metcalfe’s Law (Briscoe, Odlyzko, Tilly, 2006) (value or “effectiveness” of a network increases to the square of the number of users of the network) by the NCW proponents, their critics insist that advocates of NCW erroneously treat the number of transactions on the network as a source of power and advantage. Even more, practice shows that real networks have certain saturation threshold, when network congestion, due to the growing number of transactions, will force the value curve to flatten and decline (Giffin, Reid, 2003a:21). The NCW thesis is also accused as influenced by naive inductivism (Nola, Irzik, 2005:207-229); therefore the tenets of NCW are formulated on a methodological basis of non-scientific approach. As a result, the tenets are criticized that robust networking is not defining the quality of information sharing; information sharing and collaboration doesn’t necessary lead to right conclusions and decisions; and shared situational awareness is “neither a sufficient nor necessary condition for the behaviour described as self-synchronization” (Giffin, Reid, 2003b:18).

Professor Milan N. Vego from the U.S. Naval War College argues that there is no proof that Network Centric Warfare will be effective in fighting a strong and well prepared opponent. Recent conflicts, where the United States were involved and where, according to the concepts’ proponents, elements of the concept were successfully tested, took place against relatively technologically weak enemies such as the Taliban and the Iraqi forces. On the other hand, fighting counter-insurgency operations in Afghanistan and Iraq have proven how small is the potential that the networking of force can provide in finding and eliminating insurgents. According to Milan Vego, the recent U.S. experience shows that small and dispersed forces will not be able to control occupied territory and its population. It is mentioned that suggestions to conduct joint operations at lowest possible levels (self-synchronization) will result in increasingly complicated coordination between elements of different services and extended time to plan joint actions, because each service has its specific command and control process and logistic. He is also pointing out that, despite the emphasis on a human dimension by the proponents of

Network Centric Warfare, the concept itself, however, is mostly dealing with information dominance and technological factors (Vego, 2007).

Jeff Cares, the author of “Distributed Networked Operations: The foundations of Network Centric Warfare”, in his interview to *The Journal of Electronic Defence* (Cares, 2006:38-40) underlines that, under the cover of the NCW implementation, large amounts of funds have been already spent, but the aim to be achieved is not clear, and any visible return of investment could not be observed. He also argues that an idea to have a vast number of interlinked battlespace entities makes network arrangements very complicated, and current technologies are yet to be capable to cope with this issue. In his opinion, the NCW concept doesn't clearly articulate what are the mechanisms of networking advantage. Jeff Cares states that even when all the necessary information is present on the network (for instance, in a huge scale central database), there will be no tools to select information relevant to a particular battlespace entity in a particular situation, because it is not realistic to develop queries supporting retrieval of relevant information in a very dynamic and unpredictable military environment.

Col. Alan D. Campen, USAF (Ret.), in his article is sceptical about the practical proof of the NCW concept presented by its proponents: “Probing questions about NCW were raised as early as 1998 and are echoed today by other voices who contend that substantial technology-driven changes in force structure, organization and operational art should be founded on more substantive evidence than can be gained from selectively sampling the scenario-unique sands of the Iraq War. Fixation on battlefield experience in Iraq can mask issues that rival NCW in fuelling the engine of military transformation” (Campen, 2004). He is supported by Greg Grant, whose opinion is that experience in Iraq has proven that less technically advanced adversary can apply time-tested concealment methods and cheat state-of-the-art U.S. sensors. Grant also explains that, in situations when the enemy becomes out of reach of the U.S. sensors' view or when communication with the sensor is degraded, the enemy position becomes halted on the information system screen because there is no more updating feed from the sensor. In this quite frequent scenario, relevant situational awareness could not be produced (Grant, 2005). The potential danger of specialization of platforms (sensors and actors) could put actors into danger when communications are lost or degraded by the enemy, because

in this case actors become blind: “As fighting vehicles - planes, ships, tanks - are connected to the web, they tend to be dumbed down to save money. Why carry a sensor when the same information is available from other sources? But if network access is severed, the vehicles may lack the capacity to autonomously defend themselves.” (Thompson, 2003)

Aldo Borgu raises a number of conceivable issues related to the practical implementation of Network Centric Warfare. For instance, it would be a challenge to establish a single network across different services and nations. In his opinion, it most probably will be difficult to integrate “network of networks”. Extensive sharing of information has potential danger of information overload and decreased speed of command. On the other hand, access to the same, even high quality, information doesn’t automatically mean that different people will come to similar conclusions. In reverse of a Network Centric Warfare proposition of decentralisation of decision making, there is a great deal of probability that availability of low tactical level information for the highest levels of command may lead to even greater centralization (micro-management). He also points out that different nations have different view and different approach to the network related military concepts, which automatically implies problems with operational and procedural interoperability. Fast technical U.S. advance will even deepen capability gap between the United States and its allies, so Network Centric Operations in coalition may have no common technical basis (Borgu, 2003).

2. Networks

The “network” is an essential part of the Network Centric Warfare concept and, in a broad sense of its meaning, is regarded as a combination of wide spectrum of links between various geographically dispersed entities assembling them into a single enterprise (Alberts, Garstka, Stein, 1999:115-116). With respect to operations, we can distinguish two types of networks – those of technological nature (linking equipment, providing communication means and virtual collaborative environment for actors and decision-makers), and intangible networks between people within military enterprise (between individuals in a given organization and between different organizations). In this section, I propose analysis of potential challenges for multinational military enterprises to establish and exploit

communication networks from a technological standpoint and leave human dimension of the networks for the last section.

2.1 Availability and interoperability

The robustly networked force is the first prerequisite, necessary for realization of the Network Centric Warfare tenets. Taking into account geographical dispersion, this force could only be created with the existence of appropriate interoperable communication systems (Alberts et al., 2001:107). The first and foremost issue with implementation of the Network Centric Warfare concepts in the multinational environment is the lack of networks, deployed by coalition members, especially from the nations having small armed forces, small defence budgets and, as a consequence, no or small scale national network-centric programmes. In addition, even “big nations” (such as the UK, Germany, Canada and others), when comparing their potential capabilities to deploy to the theatre of operations with the present U.S. capabilities, are far behind the latter (Luddy, 2005:14). The current state could be illustrated by a felicitous remark of Duncan Hunter, Chairman of the Armed Services Committee of the U.S. House of Representatives, when he compared the situation of sharing the financial burden within NATO to a picnic in which the U.S. “provides the T-bone steaks while some other countries bring the plastic forks and some just show up with a smile” (Trowbridge, 2006). This also perfectly applies to nations’ investments into reliable deployable military communications systems (Spierling, 2004:453).

To realize the main idea of the first Network Centric Warfare tenet, to establish networked forces and improve information sharing, the network services should be available theoretically wherever the operational situation demands; however, robust network connectivity down to the tactical level is still the issue to be addressed in the U.S. armed forces themselves (Tisserand, 2006:B-2). Usually, at the low tactical level, national communications systems can provide only voice communications, which is clearly insufficient for intelligence information distribution, targeting data and higher commander’s intent delivery. The most promising way to provide all necessary types of communications services (voice, data, videoconferencing etc.), is to use satellite communications, but again it is a scarce resource even for the United States, not to talk about the small nations, where national satellite communications are simply not available

and services, offered by the commercial providers, are expensive and not always reliable.

Another significant issue is that today, for multinational operations, the nations are deploying their communications systems which cannot be interconnected due to the use of different protocols, bandwidths and frequencies. Interoperability has been on the list of unresolved issues for a long time, even in those organizations which work hard on achieving interoperability among its members. NATO could serve as a typical example: “The performance of the European armed forces in NATO - or U.S.-led coalition operations, such as in Kosovo, Afghanistan and Iraq, demonstrated clearly the existence of a glaring transatlantic capability gap that has limited the interoperability of multinational forces and the efficiency of coalition war fighting” (Nolin, 2006).

Despite the growing trend to build their networks in accordance with commonly agreed military standards, the nations continue to realize their specific national approaches even in those cases when the agreed standards (for instance, NATO STANAG's) are taken as a basis. Quite a promising direction is the adoption of commercial standards in the military world (Commercial Off-the-Shelf, or COTS, solutions); however, within the industry we can notice a variety of proprietary features, on top of commercial standards, which make network solutions, delivered by different manufacturers, not interoperable, although those solutions are based on the same commercial standard. Lessons learned during multinational military communications and information systems interoperability exercises show that the United States and European nations are still quite away from the “plug and play” level of communications interoperability.

2.2 Management

Having the national networks deployed and getting them interconnected is not the end of the story – usually real operating environment demands the ability to flexibly reconfigure the network, provide increased bandwidth between particular nodes on the network or connect new nodes to the network. Multiple nations, operating in a relatively small area, have diverse requirements for the use of electromagnetic spectrum, necessary for operation of their sensors and wireless communications. This is all about

the network management. Taking into account the growing bandwidth demand, it is most likely that opportunities, provided by rather rapidly evolving communications technologies, will be behind the user requirements. Therefore implementation of the net-centric concepts would require an efficient use of network resources, and this is the place, where network management will play its very important role.

Network management within national domains is quite a challenging issue (Donnelly, 2005). However, within the multinational environment, it requires even more effort. First of all, in the recent years, we cannot observe any significant improvement in defining multinational networks' architecture. For instance, NATO Consultation, Command and Control Board and its sub-committees are working on NATO Information Infrastructure (NII), which is supposed to address the Alliance's Network Enabled Capabilities architectural issues, but at present stage, it doesn't seem that architectural developments are turning towards the real net-centric approach. On the contrary, we are still discussing the issue how backbone network, which is supposed to be provided by NATO, will be interconnected with national "appendixes"; therefore hierarchical network architecture is still in place (CNSSC, 2008). Continuing with this approach would not contribute to the construction of flexible and dynamic networks, where a network participant can communicate with any other wherever it is located and whatever nation it belongs to. How can we imagine communication in a hierarchical network between an airborne platform from nation A and a ground-based unit from nation B, when that platform was re-tasked on the spot to accomplish the mission in the airspace over a ground unit, if co-ordination didn't take place between nations A and B in advance? These issues were already identified during real operations (Hayes, 2004).

Similarly to networking solutions themselves, nations usually have their nation-specific approaches to the network management, consisting of a variety of methods, tools and technical solutions, because there is no multinational consensus how to manage multinational federation of networks, or, in case of the network-centric approach, the single network made of national "pieces". This happens because we are still thinking in the hierarchical network architectural dimension.

Network, truly supporting net-centric approach, has no centre. In a single nation case, it is possible with current technologies to construct the network, made of self-managed nodes, but there is no commonly agreed technology in place today, supporting management of a multi-domain network, where constitutive elements are based on different technology. To illustrate the situation in an even more realistic way, it should be stressed that nations are usually deploying not a single national network, but a number of networks to support different services (Army, Navy, Air Force), different functional areas (intelligence, logistic, command and control), and different classification domains. Therefore co-ordinated network management doesn't look very much realistic. "One analysis of CENTCOM operations in Afghanistan and Iraq that year noted that American planners were dealing with more than 84 different coalition networks. ... Needless to say, interoperability between this wide variety of networks was extremely variable, and mostly non-existent. As such, information exchange between members of the coalition was often a sluggish affair" (Mitchell, 2006, p. 54).

Inconsistency in national network management solutions could be illustrated by the following example. Informational advantage primarily is facilitated by sharing real-time information among the members of the coalition (Alberts, Papp ed., 2001:258), which in turn can contribute to the achievement of the desired military effects. However, without the co-ordinated network management, it would be hard to achieve the "identical real-time", i.e. in the multinational environment, every national domain might have its own "current time", not necessarily matching with the current time in other nation's domain. These time differences could produce a vast impact on the quality of certain processes, such as tracking of an adversary's fast-moving platform by one nation, then sharing track information and expecting the engagement of that platform by another nation.

2.3 Protection

The last, but definitely not least, issue concerning coalition networking is effective protection of networks. Without it, network's survivability cannot be assured. As a result, in a combat situation, the unprotected network will not live for long, with all resulting consequences. It is underlined in the U.S. Department of Defence Transformation Study Report that "NCW

offers the potential for dramatic advantages, but carries the risk of a major loss of capability if our networks are penetrated or significantly disrupted” (Transformation Study Group, 2001:29).

The main threats to the communication systems are coming from their vulnerabilities to physical attacks (communication nodes and wired communication lines), degradation of network performance (jamming, interference), and unauthorized access (eavesdropping). Computer networks are vulnerable to cyber-attacks such as insertion of malicious software, computer viruses, unauthorized access to the computer-based systems etc. Military communication systems are not an exception, thus are exposed to various attacks as much as civilian ones. It is obvious, that technologies nowadays are spreading very fast, therefore quickly becoming available to our present or potential adversaries too (Alberts, 1996).

Military network protection technologies, currently used in the United States and most of the European countries, are based on electronic counter-countermeasures (frequency hopping, spread-spectrum technologies), encryption of communication links, and computer network defence systems like firewalls, intrusion detection systems and anti-virus software. Today, quite an impressive arsenal is available to protect our networks; however, within the multinational environment there are numerous challenges to protect the entire coalition network when it is made of national segments. The first challenge which future coalitions will face is about the different level of technological advance in general, and in the network protection technologies in particular. This issue can be observed currently due to uneven defence expenditures, time-divided defence modernization programmes or diverging priorities. The consequence of this aspect is the inadequate protection of different national networks, which precludes coalition partners with better network protection from connecting their networks to the nations with less protected networks. The second challenge, even among most technical advanced nations, is incompatible national solutions of the network defence. Currently, almost every nation implements its proprietary solution, which is not in favour of passing the necessary information to another nation (Networking Working Group, 2008). When, in static networks, various gateway solutions could be applied, it still would be a challenge to pass the information from one platform, belonging to one nation, to another platform from another nation in a very dynamic environment that

a networked coalition is supposed to be. It is simply not possible to predict who is going to talk with whom and, even more, to design working solutions for all possible situations in a net-centric self-synchronizing environment.

The current situation and at least mid-term trends could be illustrated with the following example: NATO as the biggest modern military alliance has certified several encryption devices; however, those devices are used mostly in NATO networks or in those cases when national military networks should be interconnected with NATO ones, whereas many of the NATO nations, within their national domains, continue using their nationally approved and not always compatible encryption devices (Leschhorn, Buchin, 2004). In case of the same encryption devices that various nations supposedly can possess, it doesn't solve a problem, because crypto algorithms may differ, and crypto key management within the national networks is solely a national prerogative and responsibility.

Mutual trust and political disputes among coalition partners obviously is not a technological issue, however it may heavily impact building coalition networks as such. Political attitudes of one member towards another certainly is not precluding any given nation to execute the research, development and implementation of advance interoperable communications solutions, but definitely affects transfer of know-how and technology between coalition partners. As it was mentioned above, different nations have unequal level of defence expenditures. Without sharing knowledge, it is not realistic that nations even theoretically can reach similar level of technological advance, so coalition-wide networking may not happen due to uneven technological development. Another politically-driven issue is that frictions between various nations are reflected in their willingness to share the information. For instance, quite recently Turkey objected of NATO sharing information with the European Union, mainly because of Cyprus' membership. Despite that the official reason was that Cyprus is not a Partnership for Peace nation, it is obvious that it was not the essential reason to obstruct sharing intelligence information with the EU (Dempsey, 2007).

3. People

As it was previously discussed, successful realisation of the network-centric concepts should be enabled by highly interoperable technical infrastructure. However, in its essence, it is very much dependant on an effective interaction between the people. Diversity in international enterprises nowadays is a reality; therefore military coalitions are not the unique case. But I would argue that it is one of the most extreme cases in terms of the complexity of the environment itself (Cares, 2005:39-49), need for high-performance, unambiguous comprehension of dynamic situation, expedient decisions and appropriate precise actions.

NCO, by the name itself, imply a high degree of networking, but “the implementation of NCW is first of all about human behaviour as opposed to information technology” (Office of Force Transformation, 2005:3), which means that, in order to have an advantage over our adversary, we have to share the available information across domains of the military enterprise, make decisions and operate faster than our adversary. In other words, the efficacious teamwork is the most crucial and demanding objective we have to achieve.

Military operations in multinational coalitions are a far more complex issue than single-nation operations, due to the unavoidable different procedural, educational and perceptual backgrounds, which in many cases cause misunderstanding and frictions; therefore possible effects of national and, thus, cultural diversity on the implementation of the network-centric concepts in the coalition environment should be evaluated. In this section, I first suggest to analyze knowledge creation processes in deployed dynamic multinational military teams and identify potential issues affecting their performance. Later, I will turn to the effects and implications of cultural differences between nations, then shortly touch upon the intervening factors such as organizational culture and cognitive diversity.

3.1 Knowledge in multinational teams

Multinational personnel form and most probably will continue to form a basis to sustain multinational headquarters and units. It is a prerequisite for Network Centric Operations that multinational formations should maintain a high degree of situational awareness (knowledge of situation) and the

ability to co-operate within the team and with other teams in the military enterprise. In order to fulfil this mission, personnel should be conversant with team's internal and enterprise-wide working procedures. In other words, every member of the team should have the same basic knowledge of how his multinational formation is functioning. Beside official policy and rules, as time goes, most of military organizations, regardless of their size, develop and maintain unofficial "code-of-conduct", comprising Grundyism of relations between team members, practice-proven courses of actions within certain situations and unique interpersonal affiliation.

When a new person joins the organization, it is obvious, that he or she needs certain time to adapt to a new environment in order to become a full-fledged team member. The more the new environment is different from that already experienced or expected, the more time is necessary for adaptation and reaching the state of ability to efficiently contribute to the teamwork. When, after a certain period of time, the same person leaves the team and organization, "his departure may reduce that organization's collective knowledge more than if its internal training manuals were lost" (U.S. Joint Chiefs of Staff, 2005:10).

Now, let's take an example of a given team dynamics in the multinational military Peace Support Operation (PSO). Troop-contributing nations normally send their personnel for various time-frames, depending on many factors, such as climatic environment, intensity of the operation, and nature of the position that certain person is supposed to fill. I would argue that most nations stick to the half-year average of the rotation cycle. It doesn't, however, mean that if nation is contributing the personnel to different positions in the same mission, all personnel will be changed within the same rotation cycle. If we have a team to which several nations are contributing military personnel with their national duty periods (rotations), it results in a very dynamic by its composition organizational element because of the overlapping national, usually not aligned, rotation cycles. I would like to stress that this is a common practice rather than the exception in the current operations in Iraq and Afghanistan.

For exploiting the promises of Network Centric Warfare, every individual within the team and the team as an organizational cell itself should develop, maintain and share situation awareness, or knowledge, which is meaningful in daily military business – analysis of situation and possible actions'

alternatives, decision-making, command and control, targeting and engaging the targets. In order to better understand how organizational knowledge is developed and maintained, let us take SECI (socialization, externalization, combination, and internalization) spiral model (Nonaka, Toyama, 2003:2-10). The organizational knowledge-creation theory distinguishes two types of knowledge – explicit and tacit. Explicit knowledge comprises the known things that we can express in a written form and share with others; it is based on knowledge of rules and definitions. Tacit knowledge is about the personal experience, know-how, skills and intuition – those “things we don’t know that we know”. According to the theorists, “... tacit knowledge is produced by our practical consciousness and explicit knowledge is produced by our discursive consciousness” (Ibid:4). To make a long story short, I just would like to briefly present the process of creation of knowledge, which involves four phases where knowledge is converted from one type to another.

Socialization phase involves creating new tacit knowledge and sharing it with other individuals within the team through daily social interactions. During the externalization phase, tacit knowledge of every member in the team is articulated within the group and, in the process of synthesis, is converted to explicit knowledge. Explicit knowledge, created within the given team throughout the combination phase, is combined with the explicit knowledge, created by other teams in own organization and other organizations. Then this knowledge is combined across the organization and becomes organization’s explicit knowledge. It automatically implies interactions between the teams in organization and between organizations. Organizational explicit knowledge in the internalization phase, via daily exercising, is converted by individuals to tacit knowledge, which then is applied in routine work. The last thing which should be mentioned here is that four phases of knowledge conversion amplify the level of knowledge itself; therefore graphical representation of tacit/explicit knowledge conversion process is not a circle but an expanding spiral (Nonaka, Toyama, 2003:5).

Putting team dynamics and knowledge building continuum together, I would argue that, in case of dynamic multinational military teams and organizations, it might be very probable that frequent change of team members would have a negative effect on the overall team performance in general, and on development of situational awareness in particular. Here by

situational awareness I mean not only relatively instantaneous awareness, widely discussed by advocates of the network-centric concepts, but the overall military enterprise situation awareness through the entire period of military operation. Creation of adequate level of knowledge (or awareness) within the team requires certain time; even longer time is required to share the awareness between the teams and develop organizational awareness. I would suggest that current multinational personnel rotation practice does not give the sufficient time for this. One could argue that military personnel is coming to mission areas already trained and prepared to work in tense military operation environment within multinational enterprise; however, I would like to mention that, first, even the most realistic training could not encompass all uncertainties of real life; and second, tactics, techniques and procedures for conducting Network Centric Operations are yet to be developed, therefore nobody knows whether the NCW doctrine will be present in all troop-contributing nations and, if so, would it be an interoperable doctrine. Situation becomes even more complicated when geographically dispersed virtual teams are coming to the scene (Alberts, 2002:135) – absence of face-to-face human interactions may have an uncomplimentary effect on knowledge conversion between tacit and explicit.

3.2 Cultural diversity

Previous part discussed the impact of constantly changing composition of teams on the capability to develop situational awareness within the team and across the organization to which that team belongs. However, as probably noticed, multi-nationality was taken into account only to demonstrate its influence to the teams' dynamics. Gradually adding the colours to the picture, here I would like to introduce one more dimension – cultural diversity among the members of multinational teams. One of the most famous researchers and theorists in this field, Geert Hofstede, argues that "... people carry „mental programs“ that are developed in the family in early childhood and reinforced in schools and organizations, and that these mental programs contain a component of national culture. They are most clearly in the different values that predominate among people from different countries" (Hofstede, 2001: xix).

According to Hofstede, "collective programming of the mind" (Ibid:9) is what makes groups of people different and could be called as a culture.

Hofstede has suggested to present nations' cultural differences in five dimensions: power distance, uncertainty avoidance, individualism versus collectivism, masculinity versus femininity, and long-term versus short-term orientation (Ibid:29). NATO and EU nations, in three dimensions identified by Hofstede (individualism vs. collectivism, masculinity vs. femininity, and long term vs. short term orientation), from my point of view, either look very close to each other² or cultural diversity's effect on information sharing, collaboration, and self-synchronization is not evident. For instance, in case of individualism/collectivism dimension, most of the western (North America, Europe) nations belong to the group with high Individualism Index (IDV) (with the exception of Greece and Portugal), therefore I don't expect (and, in fact, I have not experienced) significant cultural differences in this dimension. Taking this into account, from here I suggest taking a look at how national differences in power distance and uncertainty avoidance dimensions may affect implementation of the network-centric concepts in practice. Referring to the tenets of Network Centric Warfare, I would like to analyze how cultural diversity may affect information sharing, collaboration, and self-synchronization (readiness to decide and act without superior's intervention) as well as readiness to integrate into so-called "edge organizations" (agile organizations with flattened hierarchical structures) (Alberts, Hayes, 2003:215-221).

Power Distance is a dimension, measuring interpersonal power or influence between superior and subordinate in terms of subordinate's perception (Hofstede, 2001:83). Characteristics of cultures with high Power Distance Index (PDI) (France, Turkey, and Belgium) are: centralized decision structures and more concentration of authority; tall organizational pyramids; reliance on formal rules; subordinates expecting orders; efficiency is achieved by authoritative leadership; and exchange of information is constrained by hierarchy. Characteristics of cultures with low PDI (Scandinavian countries, the UK, Germany, the United States) are: decentralized decision structures and less concentration of authority; flat organizational pyramids; reliance on personal experience and subordinates; subordinates are expecting to be consulted; efficiency is achieved by consultative leadership; openness to exchange of information vertically and horizontally³. I would argue that representatives of the first group (high PDI) would have more difficulties to realize the NCW tenets in their national organization and will be less capable to integrate themselves into networked enterprises, less willing to share the information

horizontally as well as to take self-synchronization initiatives without superior orders. Conversely, the representatives from the second group (low PDI) are more psychologically prepared to implement sharing of information, collaborate with peers and take the initiative, when the situation demands.

Uncertainty Avoidance is „the extent to which the members of culture feel threatened by uncertain or unknown situations“ (Ibid:161). Nations with the high Uncertainty Avoidance Index (UAI) (Greece, Portugal, Spain, France) are: affected by fear of failure; prefer to take tasks with sure outcomes, no risks and following instructions; are enthusiastic towards technological solutions; innovators feel constrained by rules; top managers are involved in operations; power of superiors depends on control of uncertainties; conceptions of management are highly formalized; are task oriented. Countries with low UAI (Denmark, Sweden, the UK, the United States, Canada) are: tended to hope for success; prefer to have tasks with uncertain outcomes, calculated risks, and requiring problem solving; are sceptic about technological solutions; innovators feel independent of rules; top managers are involved in strategy; power of superiors depends on position and relationships; ambiguity in structures and procedures is tolerated; are relationship oriented. Taking the mentioned characteristics into account, I suggest that representatives of the nations with higher UAI will more carefully analyse incoming information before taking decisions (probably more time for decisions will be necessary), will react rather than act, and rely on communication networks and information systems. Personal initiative in these nations is more suppressed by the rules, and there is probability of micro-management instances. This brings me to the conclusion that, in “high-UAI nations”, self-synchronization shouldn't be most preferable way of conducting military operations; however, what concerns the technological side of the network- centric concepts, these nations should be keen to implement it. National group with low UAI are more eligible to perform Network Centric Operations in a self-synchronized way, but will not heavily rely on technologies.

Ethnic or national dependence is not the only factor influencing cultural diversity. Other factors, such as organizational culture, make a big influence on individuals' values and perceptions. In case of multinational military teams, the good news is that all members belong to the same military cultural group. The bad news is that military organizations in

different nations maintain their own organizational culture, which after additional research surprisingly may appear even more influential than national culture (Hagen, 2006:90). Even more, each service (army, navy, air force) maintains its unique organizational culture. Therefore, here is a big potential that this type of cultural pattern may as well have an impact on readiness to share information, co-operate with other services and act without given instruction in concert with other units or teams.

While Hofstede is mostly oriented towards cultural differences and their influence on values, other authors identify behavioural and cognitive facets (Klein, Pangonis, Klein, 2000). While behavioural differences among different nations are easily recognizable, differences in cognitive field in most cases lack research mainly because of the risk of being accused of promoting national and racial inequality. However, I argue that differences in cognition, despite their intangibility, impact building of shared situational awareness, because the same phenomenon may be perceived by different cultures differently. Therefore, situational awareness as such and actual understanding of the situation may be perceived differently by representatives of different nations. To avoid any misunderstanding, I don't say that some cultures are smarter than others – I simply say that the way of thinking differs, and different conclusions and decisions can be drawn from the same information.

Conclusion

The purpose of this article was to define some factors, influencing implementation of the Network Centric Warfare concept in the multinational coalition environment and to identify possible NCW implementation challenges.

First of all, discussing the present status of the Network Centric Warfare concept, we have to admit that the concept is still lacking theoretical argumentation and confirmation by valid empirical results derived from experimentation and real life experience. The current NCW theoretical basis as it is presented by its proponents in the form of not widely accepted New Economy Theory and reliance on questionable interpretation of Metcalfe's Law has a discouraging effect not only amongst the potential allies, but also within the significant part of the U.S. military community.

The postulates of the NCW tenets had raised certain doubts whether their logical chain can be accepted as an axiom, because it is not obvious and not yet practically proven that networking itself will lead to qualitative sharing of information, which in turn would result in right military decisions and common understanding among coalition partners. Mentioned doubts, along with uneven technological advance, probably were the main reasons why other nations just not “jumped to the U.S. train“. They rather induced the allies to take different national approaches to the network-centric military concepts. In case of further, purely national, development, the divergence of approaches would lead to the potential reduction of doctrinal, procedural and technological interoperability, which in turn decreases probability that Network Centric Operations in the coalition environment have a chance to happen in the future. NATO Network-Enabled Capability as a multinational initiative has the potential to provide the framework for the coordination and alignments of national developments, but its official three-year old history has not demonstrated great shifts in this direction yet.

Secondly, the already mentioned different speed of technological advance among potential coalition partners and existing, if not growing, military capability gap between the United States and its European allies reduce the possibility to construct a ubiquitous, seamless and interoperable coalition network infrastructure. The demand to build deployed coalition networks may, first of all, face the mere absence of capability among less economically developed nations to bring the adequate equipment to satisfy their own military requirements; therefore, their ability to contribute to the coalition network grid is even more doubtful. This will eventually lead to division of the nations in the coalition to those substantially contributing and those again taking a “free ride“. The worst situation that could happen is that some of the nations with their troops will find themselves out of coalition network coverage. The consequences may vary from the absence of situational awareness to “friendly fire” incidents or collateral damage.

Although most of the coalition members will manage to deploy sufficient number of equipment, it is not the end of the story. The past and recent experiences as well as future trends demonstrate that still a lot has to be done in order to interconnect national networks and make them transparent for the uninterrupted information flow between the members of the coalition. The main reason for this issue is a variety of national

military requirements and industry driven proprietary solutions, caused by notorious reasons such as uneven technological advance, availability of defence funds and lack of interoperability standards. Different and not always interoperable national approaches to network architectures, network management solutions and network protection techniques and procedures will continue to be a serious obstacle to conducting coalition-wide Network Centric Operations.

It should be underlined, that one more issue causing troubles in the multinational physical networking domain is not actually technological at all. Various bilateral political tensions and disputes among potential coalition members lead to finding various good reasons to not interconnect their networks whatsoever and to the absence of will to share the information, which may be vital to the peer in coalition. Military usually have no instruments to overcome this issue on their level – it is solely in the hands of politicians, therefore the problem will continue to resurface.

Thirdly, the current trends of Network Centric Warfare development show that, in most of nations, the main effort was put to the technological side of implementation, while human dimension is not sufficiently taken into account. The industry more than enthusiastically welcomed the introduction of NCW by throwing a vast number of “network-centric” solutions to the market. However, this enthusiasm has overwhelmed our minds with technological direction and obscured the human being as the strongest and, unfortunately, weakest element of any warfare, including the network-centric one.

Multinational military operations imply relatively high tempo of deployed personnel rotation, which in turn, as discussed in this article, has a negative effect on multinational teams’ knowledge sharing and development. The flaws in knowledge development most probably will seriously affect the ability to build and share situational awareness in a timely manner, which in fact is the main prerequisite and key to success in Network Centric Operations. Insufficient time for building team cohesion will weaken the overall coalition’s ability to maintain shared situational awareness, take effective and opportune decisions and perform military actions in a synchronized way.

Cultural diversity among coalition partners influence performance of multinational military enterprises; however, currently it is one of the most neglected factors. Dimensions of cultural diversity, such as power distance and uncertainty avoidance, may have if not decisive, then at least significant influence on the ability of the representatives of various cultures to integrate into a flat-structured multinational military enterprise, accept the Network Centric Warfare concept itself, put reasonably trust in modern technologies, show the initiative and take decisions without instructions from above and maintain readiness to share the information. Underestimating the importance of cultural factors will be a serious mistake, severely influencing the successful implementation of NCW concepts in the coalition environment.

It is also important to stress that different nations maintain different military organizational cultures and that their behavioural facets and cognitive patterns are not the same. Therefore, their performance indicators when acting in network-centric coalitions will differ. As a last word, I would like to say that cultural and organizational diversity as well as other specific national attributes don't mean that some particular cultures or nations are better suitable for implementing the network-centric concepts. It means that further research and careful adjustment of concepts is vital in order to acknowledge one day that the tenets of NCW work well in the multinational environment.

References:

- Alberts et al., 2001, *Understanding Information Age Warfare* Washington D.C.: Department of Defence.
- Alberts, David, 1996, "The Unintended Consequences of Information Age Technologies", National Defence University, at http://www.dodccrp.org/files/Alberts_Unintended.pdf, accessed on 07.02.2008.
- Alberts, David, 2002, *Information Age Transformation. Getting to a 21st Century Military*. Washington D.C.: Department of Defence.
- Alberts, Garstka, Stein, 1999, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd edn. Washington D.C.: Department of Defence.
- Alberts, Hayes, 2003, *Power to the Edge: Command ... Control in the Information Age* Washington D.C.: Department of Defence.
- Alberts, Papp ed., 2001, *Information Age Anthology: The Information Age Military*, Volume III Washington D.C.: Department of Defence.
- Borgu, Aldo, 2003, "The Challenges and Limitations of 'Network Centric Warfare' - The initial views of an NCW sceptic", Australian Strategic Policy Institute, at http://www.aspi.org.au/pdf/ncw_ab.pdf, accessed on 10.02.2008.

- Briscoe, Odlyzko, Tilly, 2006, "Metcalf's Law is Wrong", *IEEE Spectrum Online*, at <http://spectrum.ieee.org/jul06/4109>, accessed on 11.02.2008.
- Campen, Alan, 2004, "Look Closely At Network-Centric Warfare", *Signal Magazine*, at http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=43&zoneid=17, accessed on 10.02.2008.
- Cares, Jeff, 2005, *Distributed Networked Operations. The Foundations of Network Centric Warfare* Newport: Alidade Press
- Cares, Jeff, 2006, "The Network-Centric Craze: Will network-centric warfare really make forces faster and more effective?", *Journal of Electronic Defense*, Vol. 29, Issue 5, at <http://web.ebscohost.com/ehost/pdf?vid=1&hid=22&sid=3a5731a5-0f61-453a-920c-d454c0bfd114%40SRCMS2>, accessed on 10.02.2008.
- CNSSC - Communications and Network Services Sub-Committee, 2008, "Communications Interoperability Requirements for Operational Forces", Annex 1 to AC/322(SC/6)WP(2008)0002, NC3B.
- Dempsey, Judy, 2007, "Letter from Germany: Bickering Between NATO and EU Hampers Training of Afghan Police", *International Herald Tribune Europe*, at <http://www.iht.com/articles/2007/08/23/europe/letter.php>, accessed on 15.02.2008.
- Department of Defense, 2005, "Net Centric Environment. Joint Functional Concept", at http://www.dtic.mil/futurejointwarfare/concepts/netcentric_jfc.pdf, accessed on 07.02.2008.
- Donnelly, Harrison, 2005, "C4 Campainer. Interview with Lt. Gen. Robert M. Shea", *Military Information Technology Online*, Volume 9, Issue 5, at <http://www.military-information-technology.com/article.cfm?DocID=1024>, accessed on 07.02.2008.
- Giffin, Reid, 2003a, "A Woven Web of Guesses, Canto One: Network Centric Warfare and the Myth of the New Economy", 8th ICCRTS Conference Proceedings, at http://www.dodccrp.org/events/8th_ICCRTS/pdf/108.pdf, accessed on 11.02.2008.
- Giffin, Reid, 2003b, "A Woven Web of Guesses, Canto Two: Network Centric Warfare and the Myth of Inductivism", 8th ICCRTS Conference Proceedings, at http://www.dodccrp.org/events/8th_ICCRTS/pdf/109.pdf, accessed on 11.02.2008.
- Grant, Greg (2005), "Network Centric Blind Spot: Intelligence Failed To Detect Massive Iraqi Counterattack", copy of *Defense News* article, at http://www.oft.osd.mil/library/library_files/article_468_Defense%20News.doc, accessed on 10.02.2008.
- Hagen, Ulrich, 2006, "The Relevance of Professional Trust, Collective Drills & Skills, and Task Cohesion within Integrated Multinationality", in Hagen, Moelker, Soeters ed., *Cultural Interoperability. Ten Years of Research into Co-operation in the First German-Netherlands Corps* (Strausberg: SOWI).
- Hayes, Richard E., 2004 "Network Centric Operations Today: Between the Promise and the Practice", *RUSI Defence Systems*, Vol. 7, No. 1, at <http://www.rusi.org/downloads/assets/Hayes.pdf>, accessed on 07.01.2008.
- Hofstede, Geert H., 2001, *Culture's Consequences* Thousand Oaks: Sage Publications, Inc
- Klein, Pangonis, Klein, 2000, "Cultural Barriers to Multinational C2 Decision Making", Proceedings of 2000 CCRTS Conference, at http://www.dodccrp.org/events/2000_CCRTS/html/pdf_papers/Track_4/101.pdf, accessed on 24.02.2008.
- Leschhorn, Buchin, 2004, "Military Software Defined Radios – ROHDE & SCHWARZ Status and Perspectives", Software Defined Radio Forum Technical Conference Proceedings, at <http://www.sdrforum.org/pages/sdr04/1.6%20Business%20Models%20Cummings/1.6-1%20LeschhornR.pdf>, accessed on 15.02.2008.
- Lohr, Steve (2001), "New Economy; Despite its epochal name, the clicks-and-mortar age may be quietly assimilated", *The New York Times* at

Vego, Milan, 2007, "The NCW Illusion", *Armed Forces Journal*, at <http://www.armedforcesjournal.com/2007/01/2392378>, accessed on 10.02.2008.

¹ For a wide audience the term "Network centric Warfare" was introduced for the first time in US Naval Institute Proceedings Magazine (January 1989) by Vice Admiral Arthur K. Cebrowski and John J. Garstka in their article „Network Centric Warfare: Its Origins and Future“. A copy of this article can be found at http://www.oft.osd.mil/initiatives/ncw/docs/NCW_Origins_and_Future.doc, p. 1, accessed on 07.02.2008.

² Most of the East European nations were not evaluated by Hofstede in the 2001 or earlier editions of his book.

³ Here and further in this part, the selected characteristics are taken from Hofstede (2001).