Uroš Svete, Zoran Jankovič

Strokovni članek

IZKUŠNJE REPUBLIKE SLOVENIJE PRI UVAJANJU ZMOGLJIVOSTI OMREŽNEGA DELOVANJA

EXPERIENCE OF THE REPUBLIC OF SLOVENIA IN THE INTRODUCTION OF THE NETWORK OPERATION CAPABILITIES

Professional article

Povzetek Človeški dejavnik, tehnologija in njena uporaba ter prostor so bili v zgodovini vedno dejavniki, ki niso vplivali le na vojaško organizacijo, temveč skoraj na vso družbeno sfero. Način, kako se je informacijsko-komunikacijska tehnologija (IKT) uveljavila v vsem našem življenju, pa je resnično velika revolucija. V članku bomo predstavili to revolucijo predvsem na področju preoblikovanja sodobnih oboroženih sil ter vseh drugih akterjev sodobnih (ne)bojnih operacij v enotno delujoč mehanizem na omrežju. Zato ne govorimo več o bojevanju, temelječem na omrežju, temveč uporabljamo izraz network enabled capabilities. Posebna pozornost v članku je namenjena Sloveniji in njenemu približevanju klubu (tehnološko) visoko razvitih držav, prav tako želimo opozoriti na temeljne napake, ki so se dogajale in se še pri uveljavljanju tega dela preoblikovanja v Slovenski vojski. Tu namreč opažamo predvsem problem tehnološkega determinizma ob hkratnem zanemarjanju človeškega dejavnika, ki je (še vedno) ključni element informacijsko-komunikacijskega omrežja. Članek zaključujemo s priporočili, kako trenutno stanje ob drastičnem zmanjšanju finančnih sredstev ter gospodarski krizi optimizirati ter uravnotežiti tehnološki, doktrinarni, organizacijski ter človeški (human) razvoj slovenskih obrambnih zmogljivosti.

Ključne besede ***Transformacija, informacijska premoč, zmogljivosti omrežnega delovanja, informacijsko-komunikacijska tehnologija, tehnološki determinizem, človeški dejavnik.***

Abstract In the past the human factor, technology and its use as well as space have always been factors, which have influenced not only the military organization, but also the entire social sphere. The way in which the information and communication technology (ICT) established in our entire life is in deed a great revolution. The article presents this revolution mainly in the field of transformation of modern armed forces and all other modern actors of the (non)-combat operations into a uniformly operating mechanism in the network. Therefore we no longer talk about network based combat, but rather use the expression network enabled capabilities. The article

pays special attention to Slovenia and its approach to a club of (technologically) highly developed countries. We also want to draw attention to fundamental mistakes, which occurred and continue to occur in the implementation of this part of transformation in the Slovenian Armed Forces. It is here that we notice principally the problem of technological determinism along with simultaneous negligence of the human factor, which is (still) a key element of the information and communication network. We conclude the article with recommendations on how to optimise the current situation, confronted with a drastic decrease in financial assets and the financial crisis, and with recommendations on how to balance the technological, doctrinal, organizational and human development of Slovenia's defence capabilities.

Key words ***Transformation, information superiority, network operation capabilities, information and communication technology, technological determinism, human factor.***

Introduction

Throughout the history, the human factor, technology and its usage along with space have always been factors which have influenced not only the military organization, but the entire social environment. We can conclude, that all these three angles of an equilateral triangle are in an interactive relationship. This means that a single factor can never completely prevail, but it is true, however, that these factors take turns according to their significance.

Even though numerous technologies changed the course of events in the history, not many marked our lives in the way the information and communication technology has. If in the ninety-sixties of the previous century it seemed that this is only one of many technologies, which will be used mainly by the national defence system, the subsequent course of actions brought one of the largest revolutions in the history. Not only have the armed forces and their communication capabilities informatised (in terms of software and hardware development), the conventional weapons also got an entirely different meaning and effectiveness through digitalisation and informatisation. On the other hand, other social subsystems also informatised and digitalised, among which the most important ones are undoubtedly the economic, media as well as administrative and political social subsystems (Network Science, 2005). In the beginning of the ninety-nineties of the previous century we have, almost at the same time that the Cold War ended, stepped on the path of the information society, which is one of the main factors of the so-called modified security environment, something that almost no one forgets to mention nowadays. But what makes such a difference between the pre-information and information society, for the famous Chinese war theoretician Sun Tsu already knew the significance of information in combat? **In our opinion the biggest difference is in the amount of data and information, which we (still principally humans) are able to absorb, process, transfer and make decisions based on them.** This very characteristics of the modern society and the digital information and communication technology is what gives foundation to network operation, not only of the armed forces, but of almost all those actors, which play an important role in the modern combat and non-combat operations. It is

nonetheless indisputable that without the information and communication platform, it would not be possible to attain such high complexity in the implementation of combat operations and all kinds of non-combat activities. It is likewise indisputable that without information and communication support it would be impossible to attain the formation of task force[1], which surpasses the classical division of the armed forces on services and branches, and which can even combine parts (or the whole) of armed forces of individual states.

Within this framework, we will also highlight our central research question that we want to explain in this article. **The risk of technological determinism or the omnipotence of technology** is one of the biggest threats, which can impede the introduction of network operation[2] of the armed forces and wider. As we will demonstrate on the example of the American Army in Iraq experience, later in the article, too much attention has been dedicated to technological solutions and too little to the users of the network. And here we come to our main thesis. **Regardless of how large a system is adapted for network operation without a holistic (integrated) implementation plan, which covers both technological as well as human and doctrinal component, we will never be able to bring into effect the essence of the network, that is the shared knowledge and capabilities for the attainment of synergistic effects or the added value of individual parts, combined into a network.** Even at the appearance of artificial intelligence and increasingly numerous entirely automated processes, **it is the human, which remains the most common decision-maker and the main component part of the network.** In that respect, we believe that we should invest much more means for education and training particularly in the human. In the information societies the problem of the so-called information overload, when there is an abundance of information or even too much of information, is becoming increasingly common. The narrow throat of such network remains the human with his poorly utilized cognitive potential.

If we want to prove the necessity of a comprehensive approach in the introduction of network operation, the structure of this article has to be adapted to that purpose. The article is based on a deductive scientific analysis, which is founded on general social and technological influences on the modern armed forces. In the second part, the article continues with the presentation of the network operation concept, as it is understood in NATO. The last part of the article deals with the example of Slovenia on a micro level. This last part in particular presents an important added value, since it also uses the principle of research with participation and the constructive critical approach to scientific writing, apart from the traditional (sociological) methods of scientific writing, as for example the descriptive analysis and the analysis of primary

---

[1] *The example of the American Navy in the Enduring Freedom operation (U.S. Navy's Fifth Fleet Task Force 50 in Operation Enduring Freedom, 2007).*

[2] *The term network operation is used because the concept itself envisages much more than mere combat operations of the armed forces. These are the so-called full spectrum operations, in which, nowadays, the non-military and non-state actors participate as well.*
In compliance with the concept of network operations, all of them would be using a uniform information, communication and procedural platform.

and secondary sources. This is the only way that transition, which strives to be explicitly application-oriented, with its vision of the situation in Slovenia, can be possible. The main purpose of the article is not to describe the already known concepts, but to address the mistakes (foreign as well) made at their implementation, followed by a relatively ambitious attempt to exit the given situation by making propositions, since a great deal of attention, in Slovenia as well, has been devoted to technology and technical solutions, and too little to the human factor or to the users.

1 SOCIAL AND TECHNOLOGICAL INFLUENCES ON CONTEMPORARY ARMED FORCES

It is unambiguous that the armed forces or the military subsystem are that part of a society, which is constantly subject to transformation and reforms. It is true that in different historical periods this cycles are of various intensity, but on the other hand, we can say that in the last twenty years we have witnessed numerous revolutions (not only in military and technological affairs). The first undoubtedly refers to social changes of which the decay of numerous multinational countries is characteristic, but on the other hand we are confronted with increasingly numerous merger (economic, political and security) initiatives on local and even on global level. In many countries the social relations also changed and we can undoubtedly say that a modern state (despite a possible renaissance due to a response to the current economic crisis) is confronted with numerous challenges and actors in both, home and international scene. Some theoreticians talk about the **deetatisation** and the loss of power and monopole, which a modern state had for the last three hundred years, after the Westfall Peace, particularly in the security and military field. In short, the internal and global social changes and the changes of the security environment, dictated by both the actors as well as the security instruments and technology, have created an entirely different perception of security, into which we must unquestionably place the new types of conflicts and the asymmetric warfare. The latter is not a novelty, but it is true that, as Ivan Arreguin Toft notes in his book How the Weak Win Wars, the number of conflicts in which the seemingly weaker actors win, is rising rapidly. Why? Do we have wrong instruments for measuring power or are certain individual forms of power nowadays less useful in conflicts as they once used to be. It is true that in our time the weaker not only win numerous conflicts, but cause them as well. We can establish this by merely observing the Middle East and the operation of typical asymmetric actors, such as the movements Hamas in Palestine and the Shiite Hebsollah in Lebanon. In 2006 and in 2009, the two movements more or less intentionally provoked the Israeli intervention, at which it was clearly demonstrated that at the present time, even such superior armed forces as the Israeli Defence Forces (IDF) are unlikely to fully attain their objectives.

All these factors (social changes, changes of the security environment, joining into the alliance, new types of conflicts /asymmetry/ and technology) dictate the current transformation of the armed forces, but it is especially important for the organizational and technological transformation to accentuate the role and the significance of the

information and communication technology (ICT). Without its integral (social and technical) understanding we shall not be able to comprehend the network operation. **So the information and communication technology (ICT) refers to collecting, processing and presenting data and at the same time includes the communication element, which enables data transfer.** The data processing technology includes data fusion and their analysis as well as support in the decision-making process (Alberts, 1996; Wilson, 1998). It defines the breakthrough of the modern electronic, although principally computer and communication technology into the information processing methods. The origin of the term dates back in the ninety-seventies of the twentieth century (Bosch, 2000: 86-87), but what is essential for its wider understanding is, that it does not refer only to the technical and infrastructure hardware aspect and devices. **We must, above all, consider the aspect of software, which gives the appliances a useful value and a human factor**, which, of course, uses the software and hardware. It is therefore essential that we link the software and the hardware aspect with usage in the attainment of the desired objectives (technological utility/adaptability or the social utility). **Therefore the information and communication technology (ICT) can be defined as the ability, knowledge, skill or technique to achieve the desired effects mainly with the use of machines and appliances, enabling the information activities** (Svete, 2005: 8).

At the analysis of social dimensions of usage, above all, it is highly appropriate to distinguish between the three different aspects of information and communication technology (ICT), as suggested by Wilson (1998: 7): **The information and communication technology (ICT) as a medium, as an inserted production factor, and as a motive power of the organizational changes.** The information and communication technology (ICT) as a medium does not refer only to the contents. The broadcasted and printed messages and the programs contain both implicit and explicit values; nonetheless it is the researchers' task to infer the implicit context, which includes cultural, political and other values (worth), which are presumably a part of messages. In addition, it has to be studied whether the implicit content even came to the recipient (viewer, listener or reader), how he perceived it and how it influenced his behaviour and activity. Such flows of content are extremely important; for they can potentially influence the ethnic or social relationships, cause tension or produce cooperation.

The treatment of the information and communication technology (ICT) as an inserted part of the production is considerably different. The latter considers the information and communication technology similarly as traditional production elements (soil, work and capital), the relationships of which influence the economic production. Within this framework the most significant meaning of the information and communication technology (ICT) refers to the modification of resources, to which different individuals or groups in the society have access to, including work and capital.

The third aspect addresses the information and communication technology (ICT) as a motive power of organizational changes. In this event, the communication aspect of the information and communication technology (ICT) in particular, both within as

well as between the hierarchies, leads to the levelling of the organizational pyramids in public, private and non-governmental sector and of course also or mainly in the military organization, which wants to use the network as a spine for its operation. How have the USA undertook the introduction of such approach will be demonstrated on the example of the *Iraqi Freedom* operation. These experiences have also defined the NATO's approach to the network operation, which will also be analysed in the article.

1.1 The implementation of the network armed forces concept in the Iraqi Freedom operation

At the analysis of the use of the information and communication technology (ICT) on the side of the coalition forces, we have to highlight the critical estimations of effectiveness or successfulness of this usage, particularly at the coalition armed forces and the indirect implementa tion of military operations. Within this framework we will use the estimation presented in the document OnPoint: The United States Army in Operation Iraqi Freedom (2004), prepared by the Center for Army Lessons Learned. Talbot (2004) in the magazine Technology Review, published by the recognized Massachusetts Institute of Technology (MIT), comes to similar findings regarding the unsuccessfulness of particularly the usage of communication and information technology (ICT) in indirect combat actions.

In the document On Point: The United States Army in Operation Iraqi Freedom, the very area of informational and psychological operation or the introduction of the armed forces concept, based on the network, and informational operations in the preparatory phase of the operation and in the second phase, after the commencement of hostility, has been very critically estimated. The first critique refers to the concept of the network armed forces or the warfare. Given the decisive meaning of information for a successful and efficient operation of the armed forces, which have, apart form the human and the technological factor, influenced the outcome of conflict, in the first Gulf War in 1991, particularly after a successful use of certain information and communication systems (e.g. GPS, video, conference connections, and data processing capabilities), among American theoreticians and key decision-makers prevailed the standpoints that the very use of information and communication technology (ICT) is a key factor of America's supremacy. To this end has been developed the already presented concept of warfare, based on the network, which in stead of the traditional warfare theories (Clausewitz) uses the system theory, the theory of chaos and complexity, and warfare, the objective of which is critical (information) infrastructure nodal warfare. All types of American Armed Forces have treated the network as a key means for the supply of information to commanders and units. In this way the initiatives, such as Army Digitalisation and Force XXI (Land Forces), Effects-Based Operations (Air Forces), Cooperative Engagement (Navy) and the Sea Dragon (Marine Corps) have been formed. Despite the abundance of definitions regarding the network operation concept, it should not be confused with warfare in information systems, such as have been the most radical initiatives and plans of information warfare (in particular its cybernetic and hacker supposition), and this is

also not a case of warfare between networks of individual actors. **In this context, the network presents exclusively the way and the means for the establishment of self adaptable armed forces**, in which information sharing shall be ensured from the highest level of command down to each individual soldier in the battlefield. On the basis of such information support, each level of the armed forces or every individual within them would be able to understand the commander's intention as well as his own tactical position. In order to achieve the set objectives, the American (Land) Forces started the digitalisation of their forces already in the ninety-eighties of the previous century, but it got additional impetus particularly after 1991. In the Iraqi Freedom operation the positive influences of digitalisation on the effectiveness of force operations already manifested themselves, mainly in the understanding of the position in relation to other, own or adversary forces (situational awareness), and in addition, digitalisation also increased the effectiveness of the forces. However, numerous imperfections also came to light, due to which a complete establishment of the Network Centric Warfare (NCW) concept is not possible. One of such imperfections is undoubtedly the **interoperability within the American Forces and with allies.** If the first was a consequence of certain differences in the use of platforms; the second has been influenced by technical differences and security reasons. The land communication systems have also caused problems, as they have considerably reduced the manoeuvre capabilities. Regardless of the fact that a complete interoperability of communications, sensors and systems into a functional network anywhere in the world is difficult to accomplish, the American tendency for the implementation of network armed forces will continue in the field of education and training, doctrines, organization and leadership abilities of the command staff as well as in the development of the (information and communication) technology. **Besides the doctrinal, educational and organizational difficulties, one of the most important difficulties is also technological and technical aspect of data transfer.** The problem in introducing the tactical Internet as an information and communication basis for the introduction of the armed forces, based on networks, is the bandwidth of data transfer, something that is addressed by several authors and studies (Lettice, 2003; Moseley, 2003; Information Warfare Monitor, 2004).

2 NETWORK ENABLED CAPABILITY (NEC) AS A NEW APPROACH

If five or six years ago, we have dealt with the question of how to establish the network armed forces in the most effective way, we today prefer to discuss the network operation capabilities, which links almost all (civil, military, state and non-state) actors of modern operations.

The network operation capabilities or the Network Enabled Capability (NEC) actually signify the transformation of the alliance. We intentionally refuse to use the title *NATO Network Enabled Capability (NNEC)*, since the network enabled capabilities (NEC) are not intended merely for the NATO alliance, but, in the sense of interoperability, their purpose is to mutually connect the participants in their joint activities, regardless of their affiliation to an individual alliance or organization.

The Network enabled capability (NEC) affects other capabilities by ensuring greater quality of operations. The network operation capabilities increase the effectiveness of operation by the speed of command, accuracy, safety and the speed of the information flow, higher speed and the accuracy of the weapon system operation, improved overview of the battlefield position, surveillance over the level of task realization with the increased speed of operations implementation and by the reduction of risk and the resources consumption (Alberts, 1999: 7). They also ensure superiority of decision-making, which is defined as a state in which better solutions are passed on faster than the adversary can respond. They are a link between sensors, decision-makers and the weapon systems. As written in the Network Operations Case Study (Gonzales, 2005), the Stryker Brigade Combat Team with the Network-Centric Warfare (NCW) and RSTA[3] capabilities in organic composition, operating in conformity with the new concepts and doctrine, is incomparably more effective and efficient than a comparative unit without the NCW capability, presented by the Light Infantry Brigade. The mentioned literature is one of the rare actually performed comparisons and analysis of units capabilities, which operate in compliance with different doctrinal principles and undoubtedly manifest advantages, introduced by the NEC or NCW capabilities, as they are called in the American Armed Forces. **The NEC capabilities are a key condition for the transformation of the alliance and are crucial for the attainment of effective operation implementation, which, is in compliance with new concepts, such as the NATO Response Force (NRF) concept and the Effects Based Approach to Operations (EBAO) concept.** The NEC capabilities have a special added value in **the expedition operations** (out of area) at which the forces are geographically spread and dependant of many factors, mainly logistic and communication. They integrate different processes, form the highest – political level to the lowest – tactical, and for that reason they expressed an urgent need for the change of mentality, attained political will and obligation, which will ensure information exchange among all actors, involved in the operations implementation. With the use of modern technology, NEC enables NATO and the members of the ad hoc alliance the attainment of objectives with smaller forces. Each alliance member should define its level of commitments for the attainment of NEC capabilities with the greatest possible use of current systems. That is to say, that the implementation of network operation capability demands close cooperation of different government departments, industry and other actors in individual members, and it is also linked with considerable financial expenditures[4].

A known fact connected with NEC defence capabilities is that the alliance will provide only a small part of capabilities, while the bigger part is under national

[3] *The RSTA (Reconnaissance, Surveillance and Target Acquisition) are reconnaissance capabilities, control capabilities and capabilities for target acquisition.*

[4] *The clearest answer regarding the importance of achieving network operation capability for a successful execution of transformation is probably written in the book of the Dutch Ministry of Defence on the development of the network operation capability in Netherlands in the following words: »If you can't plug in, you can't play.« (Networked operations, The Netherlands Defence organisations steps into the future with Network Enabled Capabilities, NEC steering group of the Netherlands Ministry of Defence in Cooperation with TNO Defence, Security and Safety, Netherlands Ministry of Defence, October 2006).*

jurisdiction and responsibility, therefore it is of key importance that the members of the alliance agree upon the standards they have to comply with at the realization of national projects and the capabilities implementation dynamics.

If we address transformation in the Republic of Slovenia, which would be in compliance with the alliance transformation, in a wider context, we cannot neglect the fact that it is not only the armed forces and the defence department that are participating in its realization, but also numerous other departments, acting as stakeholders. Many members of the alliance are aware of this fact and for this reason they have introduced the management and coordination of transformation holders on a higher level. In this way greater effectiveness, interoperability and a clearer system architecture is ensured, the system of management and maintenance is simplified and the expenditures as well as the necessary personnel structure is reduced. The process is, of course, very complex and it demolishes the current "small gardens" and acquired benefits of individual structures, while at the same time, it considerably changes the processes, the doctrines and concepts.

The development of future capabilities with which the implementation of operations will be possible through the development of new concepts, architecture, standards and processes as well as connecting people, information and technologies, is of key importance for the transformation of the armed forces, capable of operating in the network operation environment. The operational demands, which will ensure more effective use of units and the battle systems, more effective logistic support and the CIMIC (civil-military cooperation) system and more opportunities for the implementation of the expedition operations, are a very important element for successful transformation.

In many cases, the interaction between NEC capabilities and transformation could be **wrongly understood and therefore inappropriately placed exclusively in the segment, which deals with transformation of the networking and information infrastructure (NII)**. It is therefore very important to ensure a comprehensive approach to the management of transformation, which will provide favourable frameworks for the operation of various holders, responsible for transformation.

NEC requires a "**from-up-downwards" approach**, which enables coherence of all activities. NEC has to be open for cooperation, not only with the defence area, but also with other structures cooperating in the alliance, for example the nongovernmental organizations, development organizations etc. The coherence of the NEC capabilities implementation is one of the main requirements for successful transformation.

The key guidelines and requirements regarding the development of network operation, which should ensure the alliance transformation, the development of NNEC capabilities, adequate concepts and the development strategy, the timeline for the provision of the communication and information technology (CIT) within NNEC and the model of the NNEC capabilities management, are written down in the NNEC

Feasibility Study, Business Case for NEC, Roadmap for NNEC, NNEC Vision & Concept, Management Approach to NNEC, NATO architecture framework, NNEC Data strategy and others, which define the approach of the alliance and the recommendations to the members regarding transformation. Due to the demand for consistency between activities for the attainment of NEC capabilities, they are the foundation of the national approach to strategic decisions for the provision of NEC capabilities in a new national environment.

3 KEY AREAS OF TRANSFORMATION

The key areas of transformation and the attainment of NEC capabilities **comprise of the areas Doctrine, Organization, Training, Material, Leadership, Personnel, Facilities, Interoperability (DOTMLPFI),** in the framework of which are presented operational demands, connected with transformation (NATO Network enabled capability (2005), Feasibility study, Executive summary, Version 2.0, 2-8). In addition, **the attainment of NEC capabilities will demand larger changes in the safety policy and in the policy of information management.**

Even though individual countries are holders of the network capabilities development, the alliance is aware of the importance of a harmonized approach. In consequence, the alliance proposes four coordination areas, »NEC Coherence Areas[5]«, for the management of key NEC capabilities. These areas present a capabilities management system and a decision-making system, connected with the attainment of NEC objectives, and also contribute to the synchronization activity. The organization of the coordination areas provides a more transparent way of capability monitoring and facilitates the management and governance of their attainment. Without an adequate management approach, there is a risk of non-coordinated operation among different holders, which manifests itself in reduced interoperability, duplication of activities and excessive use of resources. The coordination areas are:

a) **The area of operational concepts and operational requirements**, which ensures compliance of operational requirements and the NEC capabilities requirements, manifested within the framework of requirements for changes of operational concepts, doctrines and organization. It is very important that the holders of the development of doctrines, concepts and organization are familiar with key NEC ingredients and principles. The majority of operational demands are manifested within the networking and information structure (NII), which is based on Service-Oriented Architecture (SOA), in such a way, that the operational demands are manifested in the required services, which are transferred to structures, responsible for technological development. A special interaction between these two communities is essential, since the operational community often is not familiar with NEC technological advantages and capabilities. Special attention

[5] *Despite the educationally designed system and approach to NEC capabilities management, the imperfections in the current management model can be observed. Consequently, more appropriate solutions are being searched for.*

must be given primarily to interoperability on international level. In the alliance, the Allied Command Operations (ACO) play a key role in this area.

b) **The second area includes the provision of a coherent architectural development and a detailed description (specification) of services, based on operational demands.** The use of uniform specifications enables an improvement of solutions and a competitive execution and acquisition of new systems on international level. In this area the NATO Consultation, Command and Control Organization (NC3O) plays a key role in the alliance.

c) **The area, responsible for coordinating the introduction of NEC capabilities ensures coordination and the dynamics for the provision of NEC capabilities** in the framework of attaining all other capabilities or realizing programs comprising of various projects for the attainment of capabilities. The ones responsible for this area cooperate with the area for the development of operational demands and with the area for the development of technical architecture.

d) **The management and direction area** is a community, which collects and analyses information from other fields and in this way ensures the effectiveness of the decision-making system, the preparation of directives and recommendations, coordination of different recommendations, decision-making processes regarding the level of ambition, the preparation of plan documents, notification, promotion and education about NEC.

3.1 The technological foundation in the introduction of network operation capabilities

The networking and information infrastructure (NII) is a key element, providing technological interoperability of all factors in the battlefield into a uniform system and serves as a foundation for the provision of NEC capabilities.

The key purpose of the NNI is to ensure a robust, developing communication and information infrastructure between the members of the alliance, which ensures the possibility of mutual integration also between the partner states and other governmental and non governmental organizations. The NII infrastructure must provide dynamic adjustment to the needs of operation in the rapidly changing environment. The NII will develop gradually and by stages. It will include specific areas and capabilities from communication and information area, management and control area and the informational safety. The areas are described in detail in the NNEC feasibility study.

In the communication field, the influence will be expressed principally in the tendency for transition to IP networks[6], the development of the Advanced Combat Network Radio (ACNR), the Software Defined Radio (SDR), which will enable the establishment of mobile Mobile Ad-Hoc Networks (MANET), mainly in tactical environment, in which ever greater transfer capabilities are required. In addition,

[6] *The IP networks will not be able to develop independently, but they have to be compatible with the current communications solutions, such as Link 16 (Axe, 2006).*

rapid changes in tactical situation will also occur and the installment of different communication infrastructure is disabled (NNEC Feasibility study, 2005).

For the provision of long range communications capability, the network operations capability will influence the development of radio and satellite (SATCOM) HF-systems, which will increase the effectiveness of expedition operations and decrease the necessary infrastructure and the forces at the area of operations.

At the information system capabilities the influence will be observed in the development and the use of Extensible Markup Language (XML) compatible solutions and in the development and integration of systems as Service Oriented Architecture (SOA), at which the SOA presents the IT infrastructure, enabling data exchange in the business process to different applications. The information systems will also develop in the direction of optimising the solutions for work of deployable forces in tactical environment (NNEC Feasibility Study, 2005).

Special attention will be given to solutions for monitoring situational awareness, capabilities for Friendly Force Tracking (FFT) all the way to the lowest tactical levels, which will, among other data, provide the entry information for the Common Operational Picture (COP). In the field of informatisation services is required a wide spectrum of capabilities, which will enable automatisation of processes in different functional areas.

In the field of information security the capabilities development will be oriented towards a safer exchange of information among other participants (Ibidem).

3.2 Necessary functional and organizational modifications

The modifications in the concept of operations must ensure conformity of the way they are implemented with NEC enabled capabilities. An actual conformity can be seen in the achieved effects and advantages, which the information and capabilities (of sensors, weapon systems, units etc.) attain in the required time-frame of the operation. The concept, which is in compliance with NEC capabilities must be oriented towards identification, selection and the use of those own forces capabilities, which bring the largest possible effect, supremacy over the opponent and the attainment of the desired effect.

In order to provide the conformity of the development of all areas of transformation, special attention must be given particularly to the elaboration of a new units operational cooperation concept [7], which will support the effects, introduced by NEC capabilities to the greatest extent possible and adjust it to NATO concepts and develop or change the majority of field doctrines. Without the latter, the introduction of NEC

[7] *A new operational concept Stryker Brigade Combat Team (SBCT) is based on technological solutions, which enable an improved exchange of information and an operative picture of the battlefield, improve the cooperation among units, enable rapid decisions, the unit maneuver and their self synchronization, provide greater accuracy of the armed systems and finally a greater efficiency and a more successful task realization.*

capabilities is blind, lacking appropriate measures and indicators, which would demonstrate weather the transformation is going in the right direction.

We can expect modifications also in the process of command and control, mainly in monitoring of the process with a time determinant. The NEC capabilities enable a considerable reduction of responsiveness of individual systems and units and at the same time enable control of the activities realization in almost real time . In this way, the activities, which were, until now separated in time, are now joining in the command and control process, while at the same time a new, more important aspect is coming into view, that is the synchronization or coordination, which is becoming much more complex. If we concentrate on control as a time determinant, which in contents included the degree of realization of commander's decision, the introduction of network operation considerably shortened this time determinant, as NEC capabilities ensure control over realization of activities and an almost real-time decision, so that due to the dynamics of the operation implementation it is more important to ensure the synchronization and coordination in the field of operation. Due to the dynamics of the activity, the responsiveness of units and the weapon system, greater attention should be devoted to the synchronization and coordination segment in the command and control process.

The implementation of expedition operations demands a high dynamics of transferring commands and command posts as well as the reduction of forces (commands), required for the realization of tasks or for the command and control process. To achieve a certain level, essential for the implementation of expedition operations, a robust communication and information system (CIS) has to be provided within the network operation capability. The system would be reliable and would have to ensure that a part of analytical activities would take place in the homeland. For this reason it will have to be established which processes or parts of processes can be conducted or are conducted in the homeland. At the same time the headquarters procedures and the command and control concepts hve to be adequately modified and adapted.

On the basis of the developed concepts and the introduction of new technologies, all current training programs have to be modified or supplemented, not only those that designated for the use and management of individual communication and information systems.

The network operation capabilities influence the organization and formation structure primarily with automation of individual processes. If we want for the capability, built on the basis of NEC capability to obtain its effect, the organization must follow the function of an individual capability. At the installation of the organization and formation structure of commands and units, we have to establish a close connection between the concepts and processes, being implemented and the available technology. The organizational structure must mitigate and accelerate the flow of information and material for the implementation of tasks, and disable the possible occurrence of organizational obstacles or time lags, which diminish the effectiveness of tasks.

The organizational structure, built on the basis of NEC capabilities will be considerably more active (flexible, agile) than the current structures. The network operation capabilities will enable the so-called virtual operational organization, which will be designed only for the execution of a certain task or for the execution of the tasks in a certain time period (task force). Due to larger capabilities and weapon system accuracy, attained by the units with the network operation capability, the structure of individual units and the number of weapon systems, necessary for the attainment of the same effects, can diminish. The NEC capabilities as well enable the reduction of the structure of commands, since the processes, which once demanded a great deal of steps and people, are shortening and becoming automatic.

The structure and infrastructure of educational institutions has to be coordinated with the demands deriving from the NEC concept, at which they also have to be upgraded. Greater attention has to be devoted to organizational units that deal with experimentation, research and the development of concepts and capabilities.

People are the basic and fundamental part of capabilities, for they are the key element, which transform concepts into reality. People have to think in the spirit of capabilities that the network operation provides and introduces. Therefore the **education and training**, which will enable the realization of the NEC concept, is necessary. The NEC capabilities demand a change of mind and a much greater understanding of information, available to the decision-makers, of processes and tools for data processing as well as of sensors, which enable data collection. Only then we can talk about the attainment of the "decision-making superiority", which can be defined as a state in which better decisions are spread and realized faster that the adversary can respond. The new role of individual actors in the battle field and their mutual connections have to be defined. Greater emphasis has to be given to gaining peoples' trust in the C4ISR systems and information the system provides and in the tools the members use at data processing.

3.3 Exchanging information with allies – between the current necessity and the past fears

The mentality connected with information protection, deriving from the Cold War, continues to prevail. Together with the concept of operations implementation, based on the EBAO effects (Effects Based Approach to Operations), the network operation concept gives special meaning to the safe exchange of information for all, which contribute to the realization of the set goals. At the same time it has to change the way people think and tip the scale in favour of the need for the exchange of information, keeping in mind the safety features of information. The exaggeration in the information safety segment disables their exchange, which is in contradiction to the NEC concept.

In terms of cooperation of commands and units with the commands of other NATO members, of training of individuals, the reduction of expenses as well as in terms of simplification and unification of procedures, more educations on joint and expanded

computer-supported alliance exercises have to be provided, at which the feasibility of concepts is realized and cooperation of members in different tasks is provided. Due to smallness of their armed forces certain members do not have enough experience in the implementation of joint operations on strategic and operational level, but as alliance members, they will undoubtedly cooperate in commands on the highest levels as well. The system should enable access to standardized and educational contents, which the members can use for educating their staff and for preparing missions.

NEC capabilities demand technically more educated and informed staff. We do not refer only to those that will be dealing with the management of communication and information systems, but also to the users of the system services. The user should no longer be familiar only with the interface, through which he or she gets the desired information, but should have a more profound knowledge of the system as a whole. We can observe resistance to changes and novelties, introduced by technological solutions at numerous important individuals in the system. Consequently greater efforts have to be oriented towards informing about solutions that contribute effectively to the solving of tasks for which they are responsible in an individual process and to the creation of trust in technological solutions. The key problems usually do not emerge due to technology, but due to unorganised processes and unorganised data in the system, responsible for which are the users and the managers of a certain process. A tight connection between the members dealing with operational work and the development of technological solutions and those dealing with the development of doctrines and concepts, has to be established.

For the provision of NEC capabilities and the attainment of informational predomination, all units and commands as well as weapon systems must be equipped with different communication and information systems. The systems are becoming more complex and, apart form the adaptation of the structure, also demand more adequately trained staff for the management of these systems. Due to competition in the labour market, the alliance is confronting difficulties in the acquisition of staff of adequate profile and at keeping this staff in the structures. Given that the purchased technique itself does not present capability, we have several possibilities available for the solution of these problems. NATO devotes great attention to this area, also at providing staff resources, for it is aware of the significance of the contribution for the provision of the future capabilities of the alliance in transformation as a whole.

4 OBLIGATIONS AND IMPLEMENTATIONS OF NEC IN THE REPUBLIC OF SLOVENIA

At the Prague summit, in November 2002, matured the decision for transformation of the alliance forces, which will enable all kinds of operations in the new security environment. In this way, the commitment for the formation of the NATO Response Forces has been adopted. The forces will present the technologically advanced, adaptable, transferable, interoperable and endurable forces, composed of elements of all types, which would be transferable anywhere as fast as possible.

As an answer to the adopted guidelines at the Prague summit, the system of transformation objectives and the targeted areas of transformation, which would support the development of capabilities of future alliance forces, has been developed in conjunction with NNEC capabilities which support the NATO Response Force Concept. In this way, the forces would be able to perform tasks of the alliance in compliance with adequate concepts.

A NNEC feasibility study has been performed, defining the operational needs and demands with an envisaged strategy and the dynamics of changes, linked with the provision of the networking and information structure (NII) in support of transformation of the alliance and in support of the NATO network operation concept.

At the Riga summit, the efforts of NC3O for the development of NATO NNEC capabilities, which would ensure the exchange of information, reliability and security of intelligence operations as well as the protection against cybernetic attacks on informational systems, with which information predomination would be achieved, have been supported in the joint declaration and political guidelines.

The only commitment of the Republic of Slovenia, which tries to comply with the stated objectives, is the Mid Term Defence Program (Srednjeročni obrambni program, SOPR) 2007-2010, which also includes the adopted objectives, but not the ones that refer to the NNEC capabilities. The last adopted force objectives in 2008 are not a part of the applicable Mid Term Defence Program (SOPR), and therefore we are currently preparing a new one, which would also include force objectives connected with NNEC capabilities.

All force objectives propositions are oriented towards the provision of capabilities of future transferable allied forces, which will provide interoperability of national forces with other members via a timely and time coordinated implementation of objectives, for which a certain member state engaged itself. The objectives are not oriented only towards the field of networking and information infrastructure transformation, but to all areas or all capabilities. We must stress that the objectives of NEC capabilities refer to almost all other capabilities. The force objectives content, referring directly to the network operation capability for the Slovenian Armed Forces, is listed in a separate chapter. One of the main force objectives, adopted by the Republic of Slovenia, requires the network operation capabilities, in relation to their role in combat, for all Slovenian Armed Forces capabilities, more precisely for combat forces, combat support, combat service support and command support, which is undoubtedly written in the implementation requirements in the so called Capability statements.

On the whole, we can say that from the very beginning already, the Slovenian Armed Forces are in a sort of a transformation phase – technological, organizational, staff and partly functional phase (they have been transformed from a classical military organization into a predominantly expedition organization.) Numerous activities that

contribute to the development of NEC capabilities have already been carried out, but the coordination with NATO or other alliance members is also necessary.

One of the main reasons for transformation is undoubtedly interoperability in operations. Given the obligations of the Republic of Slovenia and the technological progress in the field of communication and information technology (CIT), the Slovenian Armed Forces also commenced the realization of the adopted commitments.

The alliance thoroughly addressed the task of transformation at the strategic level. It was followed by certain key documents, which clearly indicate the desired direction of capabilities development. When we pass over to the implementation level, we establish that the dynamics and the realization are more or less in the domain of individual alliance members. The demands are relatively clearly defined with strategic documents and goals, but despite the plans and the defined dynamics, they are not followed by adequate technological standards in the fields, which should be taken into consideration by all members of the alliance. Even more problems occur when we talk about standards adopted in NATO and about possibilities of their implementation in the EU, with a view to ensure the "Single set of forces" and interoperability also for those EU members that are not NATO members. The national industry of individual members and its influence on technological solutions, which later on change into standards, play the key role in answering this question. Therefore an actual competition among individual members is taking part in this field. Smaller members, such as the Republic of Slovenia, usually do not have any greater problems with this, because they are most frequently the only buyers of individual solutions of members at which this technology is highly developed. This can be either an advantage or a disadvantage. For the development of such capabilities smaller members should invest a very large amount of resources and, in addition, they are a relatively small consumer due to their size and would have problems with marketing their solutions, because of an exceptional tender. Nonetheless, I believe that the Republic of Slovenia's industry as well as its education and research institutions have a lot of knowledge and solutions to offer, but they are not sufficiently involved in or are inadequately acquainted with the possibilities of cooperation. In the Republic of Slovenia and the Slovenian Armed Forces, we have chosen a path on which we strive to follow modern technological solutions, which have already been established at one of the alliance members. **Of course, we have to stress that we refer only to technological solutions.** When we address the network operation capabilities, we have to think about the synergy of different fields that influence the transformation, and above all about the changes in the doctrine and the concepts as well as other changes, which derive from the security environment changes.

Due to inadequate understanding of transformation, the latter **has been limited mainly to technological segment of the communication and information system (CIS)** in the Republic of Slovenia and in the Slovenian Armed Forces, and is proceeding from the adopted forces objectives, which are defined as those objectives enabling greater quality of the Slovenian Armed Forces capabilities for operation. This was followed

by quite a few mistakes. The first mistake was that the introduction of the network operation capability was left to the technological segment, and the second mistake was that the other fields, essential for the introduction of NEC capabilities have not followed the technological field. These are mainly the doctrinal, organizational and personnel field. The reason because of which the objectives, which ensure network operation capability, are overlooked is that they by themselves do not ensure any capabilities even though they are represented in almost every objective or capability. **The statement, which has been written down in certain strategic documents of the alliance, referring to the fact that NEC transformation can be performed almost entirely without large financial resources is demonstrated to be wrong**, especially for those members of the alliance, which have had or have a relatively poorly developed communication and information structure. This statement will be proven true at recession, when the resources for investments and for the purchase of new systems will diminish. Desiring to provide these capabilities for the Slovenian Armed Forces, the Republic of Slovenia adopted almost all objectives, which refer to network operation capabilities, but with an incomplete analysis of the necessary resources in the defence planning process. Along with annual structure modifications and the reduction of financial and personnel resources at current financial obligations, the resources, necessary for the realization of projects deriving from the forces objectives, have been continuously diminishing. In this way, the project was brought to a standstill in the middle of the road in numerous cases of introducing information solutions. There have been several reasons. One of the key reasons was the lack of financial and personnel resources. Already for the informatisation of smaller armed forces, such as is the case in the Republic of Slovenia, a lot of resources are needed. Due to their lack and due to the fact that the NEC capabilities are provided only for a certain segment of the Slovenian Armed Forces, the interoperability problems occur already within the Slovenian Armed Forces structure, and due to the two-tire nature of modernization and different purchase rates of new capabilities or the so-called development of individual capabilities of varying speed, they occur even within the same unit, which does not present capability as a whole and which contributes only a part of its unit as a module into the capability of, for example, a battle group. This problem becomes particularly evident when we change the producer or supplier of individual communication and information solutions. Therefore the introduction of the C4ISR capabilities can present an exceptional technological challenge even within one's own commands and units due to utilized technological solutions of different generations.

For the management and the use of all C4ISR systems and for an adequate level of services of these systems it is necessary to have a highly qualified personnel[8]. The transformation into a digitalized army presents a challenge primarily or among other things also in the enlargement of the necessary number of expert personnel,

[8] *The importance of qualification is proved by the writing in the Network-Centric Operations Case Study (Gonzales, 2005: 35), which describes how the USA and the UK units have been equipped with NEC capabilities in the Iraqi Freedom Operation. Because the UK unit received the resources immediately before the operation, the unit was not adequately qualified for their use, so they transferred to the classical use of technology, without the utilization of NEC enabled capabilities.*

which professional armed forces, based on voluntariness, are having problems to provide. Beside the Slovenian Armed Forces, the alliance and most of the armies worldwide are confronted with this problem, because such personnel is very esteemed in the labour market and the armed forces usually cannot provide or keep such personnel in their lines for various reasons. **The general problems in the acquisition of personnel for the Slovenian Armed Forces taken into account, the increased demands for individual personnel profiles from the field of communication and informatics, are completely overlooked despite the expressed and confirmed demands within different projects.** The current personnel already, which has been dealing with the development and management of individual C4I capabilities, has been burdened over all reasonable limits, which caused dissatisfaction and initiated departure to other workplaces from the defence structures, or has the personnel, due to necessity to provide final operational capabilities, been transferred to other workplaces, outside the structure and units, responsible for services of communication and information systems.

Other reasons for the standstills in the introduction of information solutions are that some of the solutions introduced in the operative use have been technologically incomplete and that the processes in the defence ministry have not been adapted to new technological solutions. Problems occur mainly in the introduction of solutions on lower command and control levels. In the alliance and smaller members, which have smaller armed forces, the image of strategic, operational and tactical level of command and control can be very different. While the component command presents the tactical level of command and control in the alliance, in the Slovenian Armed Forces, for example, this is a brigade level and all that is higher is referred to as the operational and strategic level. When we talk about the tactical level in the Slovenian Armed Forces, we refer to the communication segment and the transferable radio systems with a smaller bandwidth. Informational solutions, which we have wanted to introduce on the tactical level, have not been adapted to current capabilities in the communication area. Therefore the adaptation and optimisation, which took place during the introduction of solutions into operative use, have been necessary, although they caused dissatisfaction at users as well as mistrust in the adequacy of the information solutions. Despite all that, there has not been an adequate interaction with users and their cooperation in the formation of minimal operational demands, which caused a large number of difficulties, mainly to those who were in charge only of the technological segment of an individual capability.

As already mentioned, we have wanted to accept all objectives for the provision of network capabilities, as a trustworthy partner. The consequence was the opening of numerous projects and overload of the already burdened personnel in the information and communication field. Due to the lack of personnel resources the course of the projects has not been in conformity with the planned dynamics and at certain projects, which have been mutually linked, occurred certain delays and asynchronous activity, which additionally increased time delays because of which individual solutions became too expensive or outdated and dysfunctional. Despite all of the

above, we have made the largest step in the right direction, in relation to other fields, in the technological field in particular.

At the introduction of new capabilities, the decision-makers have likewise not played their role adequately. Other than actual capabilities in the form of units that are sent to the Crisis Response Operations (CRO), the decision-makers have not been interested in NEC capabilities and in the capabilities, deriving from other objectives. In this way, the certification of individual capabilities for which it says in the capability statement that they have to ensure operation in NNEC environment, but do not fulfil this, is questionable. Undoubtedly this does not refer only to the units of the Slovenian Armed Forces. But we can nonetheless accentuate the question of measures, based on which the achieved degree of NEC capabilities in the certified units is verified.

The Slovenian Armed Forces organizational structure is constantly changing. Is it changing into a structure which will be able to upgrade and realize the capabilities and advantages offered by the network operation concept and capabilities on the basis of concepts and defined processes?

When we talk about standards, which we are supposed to take into consideration in the introduction of NEC capabilities and the adopted forces objectives, we estimate, that we also lack several other standards. In addition we witness in practice the changes of requirements and recommendations, which are not a consequence of development or the experiential learning process, but of the interest of an individual member's industry. We have especially negative experience at the latter in relation to the alliance's demand for the implementation of military information system at which the alliance is late with solutions and the members, on the other hand, adopt the solutions entirely unsynchronised, regardless of the adopted standard, which is referring to the military information system. We are convinced that all members of the alliance encounter more or less the same difficulties.

The gap between desires, commitments and resources, available for the realization of transformation and the implementation of NEC capabilities is a special problem. The desires and commitments usually exceed the actual capabilities for their realization, and therefore these commitments, in the defence planning process, are at the best, more and more frequently moving away from the promised date.

To conclude, we shall mention some experience, related to the different degree of commitments and to the implementation of NEC capabilities in the members of the alliance, which is manifested in the inadequate degree of the interoperability of units in operations. It occurs that in certain examples it is not enough to have capabilities developed to an adequate degree, since there still exist "national" safety hindrances which prevent interoperability.

The phenomenon of relying on technological solutions and the omitting of contents, which enable operation of the system even after the technology fails, should be examined in particular.

We believe that more attention has to be given to the vulnerability of modern technology and to the manners of implementing the processes without it, for without a doubt there are being developed such systems, which are directed towards disabling the communication and information systems operation.

Recommendations and the conclusion

Numerous members of the alliance have, each in their own way, started with the introduction of NEC capabilities and invested a considerable amount of financial resources into the realization of projects, which support the attainment of these capabilities. Due to the attainment of interoperability in operations performed by the alliance, high priority has to be ensured for the capabilities, which provide operation in the NEC environment. The recommendations are intended mainly for those members, which are at the beginning of the process, connected with the attainment of NEC capabilities.

The main recommendation, which has to be mentioned first, is that the commitments for the attainment of capabilities should base on an in-depth analysis and actual resources that can be provided for the attainment of NEC capabilities. During the defence planning process, special attention has to be dedicated to this question, since we ourselves decide on the degree of commitment for the implementation of the forces objectives. Industry is very aggressive in offering various "comprehensive solutions", which are to correspond to all standards, regardless of the fact that in numerous cases, these standards are not yet developed and that the solutions are still in the development phase. **We therefore recommend not to go ahead of ourselves in the introduction of solutions, which are not completely developed or are already successfully introduced in one of the alliance members.** Therefore all projects that do not lead to NEC capabilities have to be abandoned due to the rationalization of resources.

Without the necessary changes and the synchronization in the approach to the attainment of NEC capabilities in all areas (Doctrine, Organization, Training, Material, Leadership, Personnel, Facilities, Interoperability (DOTMLPFI), the introduction of capabilities will not be successful, since the mere purchase of technology does not present the introduced capability. Above all things we have to ensure the synchronization of NEC capabilities development and implementation by introducing the capabilities in other members and in the alliance.

The recognisability of NEC capabilities in all capabilities has to be ensured in compliance with the capability statement, and for each separate capability it has to be specifically defined which NEC capabilities are implemented within each of them.

At the same time has to be ensured the cooperation of all holders of various NEC coordination areas, mentioned in the article.

Due to differences in the organizations and actors, participating in the process of attaining NEC capabilities and in the process of successful integration and synchronization of their activities, the management for the attainment of NEC capabilities and the efficiency of transformation have to be brought to a higher level. The stakeholders and the key users as well as their jurisdiction and mutual relations have to be defined.

NEC brings new, technologically more complex solutions, mainly from the systems management aspect, and therefore demands a highly qualified user and manager. Special attention has to be dedicated to this field.

Vital for the introduction of NEC capabilities are the consensus of the decision-makers regarding the necessity of their introduction and the familiarisation with the acquisitions, which the organization will have benefit of due to their implementation. Without their consent and support the resources and the introduced capabilities will not be provided.

The change of mind regarding the question of information exchange is likewise extremely important. Apart form changes, essential within the framework of safety policies and the policy of information management, the way of thinking of the members, which will enable the exchange of information and mutual trust when addressing the question of their protection, has to be changed as well.

Bibliography

1. *Alberts, D. S., 1996. The Unintended Consequences of Information Age Technologies. Washington: NDU Press Book.*
2. *Alberts, D. S., 2002. Information Age Transformation; Getting to a 21st Century Military. Washington D.C.: CCRP*
3. *Alberts, D., S., Gartska, J., J., Stein Frederick P., 1999. Network centric warfare: Developing and leveraging information superiority 2nd edition (Revised). CCRP publication series.*
4. *Arreguin-Toft, I., 2001. How the Weak Win Wars: A Theory of Asymmetric Conflict, International Security, vol. 26, No.1 (Summer 2002).*
5. *Axe, David, 2006. Vital Link: A Communcations Pipeline Enables Warfighters to Do More with Less. Navy League of the United States, March 2006. Also available at http://www.navyleague.org/sea_power/mar06-32.php. 6 July 2009.*
6. *Bosch, J. M., 2000. Informations operations – challenge or frustration? Military Technology 24: 86–89.*
7. *Bucharest Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest on 3 April 2008, Available at http://www.NATO.int/docu/pr/2008/p08-049e.html 8 May 2009.*
8. *Comprehensive Political Guidance Endorsed by NATO Heads of State and Government on 29 November 2006, available at http://www.NATO.int/docu/basictxt/b061129e.htm 8 May 2009.*

9. *Gonzales Daniel, Johnson Michael, McEver Jimmie, Leedom Dennis, Kingston Gina, Tseng Michael, Network-Centric Operations Case Study, The Stryker Brigade Combat Team (2005). RAND National Defense Research Institute.*
10. *Lettice, J., 2003. "The Pentagon's tactical Internet – a war to early?". The Register, <http://www.theregister.co.uk/2003/03/21/the_pentagons_tactical_internet/> 5 September 2004.*
11. *Management Approach to NATO Network Enabled Capability (NNEC) (2007), Enclosure 1, AC/322-D(2007)0013-REV3.*
12. *Moseley, T. M., 2003. Operation IRAQI FREEDOM – By The Numbers. US Central Command Air Forces (USCENTAF).*
13. *NATO Network enabled capability, 2005. Feasibility study, Executive summary, Version 2.0.*
14. *NATO Network enabled capability (NNEC), Business Case, 2007. Enclosure 1 to 2000 SC-6 SER: NU0137.*
15. *NATO Network enabled capability (NNEC), Roadmap, 2007. Enclosure 2 to 2000 SC-6 SER: NU0137.*
16. *NATO Network enabled capability (NNEC), Vision & Concept, 2006. Enclosure 1 to 5000 SC-6 SER: NU0065.*
17. *NATO Network enabled capability, Feasibility study, 2005. Annex C to Volume II; Communication Technology for NII.*
18. *NATO Network enabled capability, Feasibility study, 2005. Annex D to Volume II; Information and Integration Services (IIS) for NII.*
19. *NATO Network enabled capability, Feasibility study, 2005. Annex E to Volume II; Information Security for NII.*
20. *NATO Network enabled capability, Feasibility study, 2005. Annex F to Volume II; Service Management Control Technology for NII.*
21. *U.S. Navy's Fifth Fleet Task Force 50 In Operation Enduring Freedom. Network Centric Operations Case Study, Department of Defense, 27 February 2007.*
22. *Networked operations, The Netherlands Defence organisations steps into the future with Network Enabled Capabilities, 2006. NEC steering group of the Netherlands Ministry of Defence in Cooperation with TNO Defence, Security and Safety, Netherlands Ministry of Defence.*
23. *Network Science, 2005. Available at http://www.nap.edu/openbook.php?isbn=0309100267, 6. July 2009*
24. *On Point: The United States Army in Operation Iraqi Freedom (2004). Fort Leavenworth, Kansas: Center for Army Lessons Learned (CALL) http://onpoint.leavenworth.army.mil/*
25. *Prague Summit Declaration, Press Release, 2002,127. 21 Nov. 2002. Available at http://www.NATO.int/docu/pr/2002/p02-127e.htm 8 May 2009.*
26. *Riga Summit Declaration, Press Release, 2006,150. 29 Nov. 2006. Available at http://www.NATO.int/docu/pr/2006/p06-150e.htm 8 May 2009.*
27. *Resolucija o splošnem dolgoročnem programu razvoja in opremljanja Slovenske vojske (ReDPROSV), Official gazette of the RS, no. 89/2004.*
28. *Srednjeročni obrambni program, Ljubljana, number 803-2/2006-58, dated 27 November 2006.*
29. *Talbot, D., 2004. "We got nothing until they slammed into us." Technology Review November 2004: 36–45*
30. *Wilson, E. J., 1998. Globalization, Information, Technology, and Conflict in the Second and Third Worlds. New York: Rockefeller Brothers Fund.*