Info-communication areas of modernizing field C2 systems and command posts in the interest of successful home defense- peace operations- and disaster-management tasks

Tibor Farkas
CIS Department
National University of Public Service
Budapest, Hungary
farkas.tibor@uni-nke.hu

Erika Hronyecz
Doctoral School on Safety and Security Sciences
Óbuda University
Budapest, Hungary
hronyecz.erika@bgk.uni-obuda.hu

Basic task of Hungarian Defense Forces (HDF) is the armed defense of our country's independence, territory, airspace, population, and material wealth – self-reliant or in allied frames – against hostile attack, and also the sharing of burden in allied settings in the creation and maintaining of international peace. Beyond these it fulfils top priority tasks during inland disaster- and other crisis situations as well. To meet these tasks with success one of the basic criteria is the complex and solid command and control capability, with a support secured by a system of advanced info-communication tools. Recent paper is meant to introduce the main trends and most important key thoughts of this development.

Communication and information system, CIS support, info-communication, modernizing

I. INTRODUCTION

Central military leadership comprises of two components: first the tasks of civilian (governmental) control over the military, which belong to the group of public service activities, and second the professional military command and control involving operational and professional leadership.

Main task of the professional leading is to meet the requirements and challenges the defense forces face, which is realized through successful command and control activity. Most of these challenges and requirements come from the mission obligations stemming from international agreements, and from partaking in the relief of inland disasters. This is prescribed in the constitution as well as other regulations regarding the HDF. In the recent years international mission activity has been shifted by task sharing in inland disaster relief and border security tasks deriving from the migration crisis.

Meeting this variety of tasks is realized with the support of military info-communication systems. This system is in basically built on a stationary network, which also in peace and period of special regulation, just as during military operations, provides analogue and digital services, secures the transmission of voice, data, text and picture (video) based information, and the access of military users to those. In the times of special regulation it enables connection to HDF field communication system thus securing an even info-communication system to evolve. These systems digitalization is the main part of the early development, evolution, which gave new solution for the leaders and users in the field of info-communication support. *Thus, digitalization not only means the technologically meant support of the so called decision circle (described above from the collection of the information to the feedback), but changes it in regarding the protocol of process as well. All members of the above network are helped by digital devices; communication between them is also secured by these. This means at the same time, that all information and transmitting regarding the given combat action appears in digital form as well, parallel or instead of the traditional documents. Occasionally this can open new horizons to the future military history research as well [1]; [2].* At the end of the nineties development of these systems began but the level and volume wasn't sufficient. As a first step the closed network was developed, when Siemens ISDN phone centers (Hicom300 E/H) have been integrated into a system. After this the so called software radios (Kongsberg MRR) have been put into service, which give an important part of the field systems. Development of other systems, field command complexes and the standardization of other tactical radios strengthened the development further, but the volume and pace of this didn't secure the base for the utilization of an entirely complex system.

In our view the most important goal of the recent reform regarding the armed forces, is to fulfil the development in accordance to the transformation of other allied nations, of which the ongoing development of deployable field command systems in a way that makes them connectable to network based warfare, a key element is.

"This article was supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences."

978-1-5386-3855-2/17/$31.00 ©2017 IEEE

II. INFO-COMMUNICATION NETWORK

Info-communication network of the HDF is built basically on three components: Fig. 1. shows these, which fulfil the info-communication support of C2 in a complex way, and get to be utilized in different ways regarding their function in each of the activities.

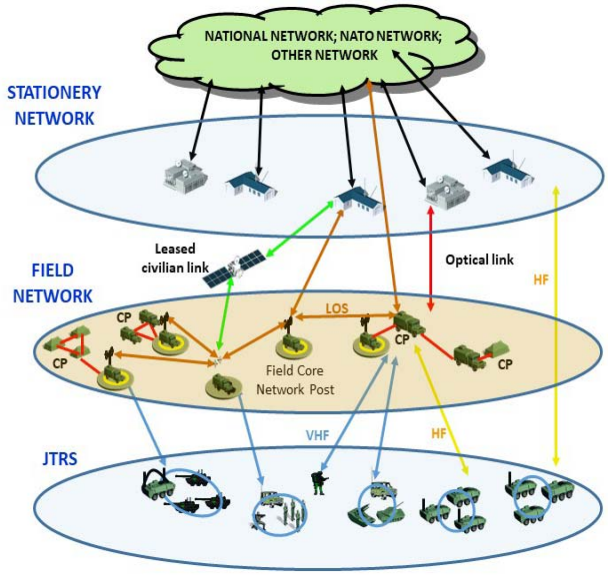

Fig. 1. Three pillars of info-communication network

The stationary network, field network, and the tactical radios (JTRS: Joint Tactical Radio System) used as part of the field network are building up the newly named ITNPG.

„According to the Act CXIII of 8 January 2011 and to the 15th §.of the Government Decree of 290/2011. (XII. 22.) Info-communications support of Operation Command and Control System of Hungarian Defense Forces (HDF) is guaranteed by the systems of Governmental Insular Telecommunication Network. As stated in the Government Regulation of 346/2010 (8 December) Hungarian Defense Forces have the right to operate an insular telecommunication network. The Insular Telecommunication Network for Purpose of Government of the Hungarian Defense Forces (ITNPG of HDF) consists of the Stationary Communications and Information System (CIS) on strategic level and mobile CIS on operational and tactical level" [3].

A. The Stationery Network

The first is a constantly deployed network, which is the platform of supporting C2 first of all in peacetime. It secures:

- The broadcasting and information support of military higher leadership.
- Technical background for C2 system work.
- Signal and IT service, meeting acquirements.
- Connecting to other networks (governmental, civilian, NATO, EU …).
- Connection of field network.

The stationery network is a multifaceted, very complex network which maintains the connecting of different network elements and transmission of data. Although it serves a narrower group of users then a civilian communication web, but its dimensions, complexity and technology can be measured to a network of any civilian telecommunication provider. The system provides integrated service, since multiple services (transmission of voice, data, weapon-control, etc.) is secured to the leadership, but it is only partly converged. Given by its functionality, it can be regarded as a complex network, where anything from MPLS (Multiprotocol Label Switching TCP/IP systems to legacy analogous centers can be found.

Regarding its components, the stationary network comprises from the following sub-networks and elements. First the Transport Network, which does the transmission, and provides connection between each points. The utilized surface can be microwave-, optical-, or copper wire network, and also connection through hired services. Second is the Traffic Management System, which is for controlling and maintaining data. Such elements are the Hicom and Hipath switch centers, and the MPLS) based network which secures data-changing. The third and last element is the Application System, applications, which are utilized by the users directly. Beyond general systems there are multiple special ones too, like GAG (Ground Air Ground), C2.

The main link for the stationery, fixed network is the microwave, LoS (Line of Sight) connection, which ensures long range and nx2 Mbps connections for different type of services. The system operate PCM (Pulse-Code Modulation) which is the simplest form of waveform coding. Fig. 2. shows the microwave network of the fixed network of the HDF [4].

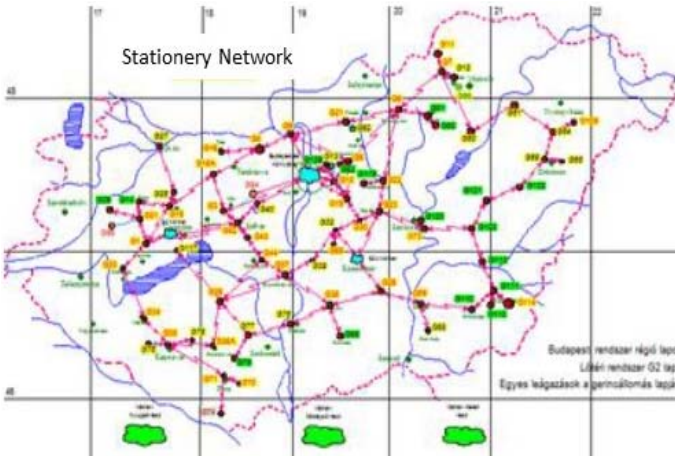

Fig. 2. Microwave links of stationery network

B. Field Network

Field signal and information system (network) is at any means utilized while tasks in other than peacetime. Its goal is to secure info-communication support for command and

control of troops, and the realization of connecting command posts. Its essential element comprises of basic signal centers, connection points in connection with each other, which build up into a transport-network, connected to which the military organizations are able to set up a complex network. Field network connects to stationary network in every case. By joining the systems, an extended network comes to life, which secures connection between the military higher command and the task force. Recently LoS connection on field level isn't secured with up-to-date digital assets.

Field networks are expanding info-communication services (video teleconference, intranet, internet, etc.) among field circumstances, thus securing access to data, and information exchange for the command. Elements of the stationary network evolve also here, the only difference is in the mobility. The standard Hipath Centre for example provides phone service for the users built into vehicles. Beyond these, other special services can also be found, like blue force tracking, which is utilized among battlefield conditions mainly. This is based on the tactical radio system. The main requirements in multinational operations– and national operations – for the field network are the essential connectivity which required down to the brigade and battalion levels. Fig. 3 shows the minimum scale of connectivity [5].

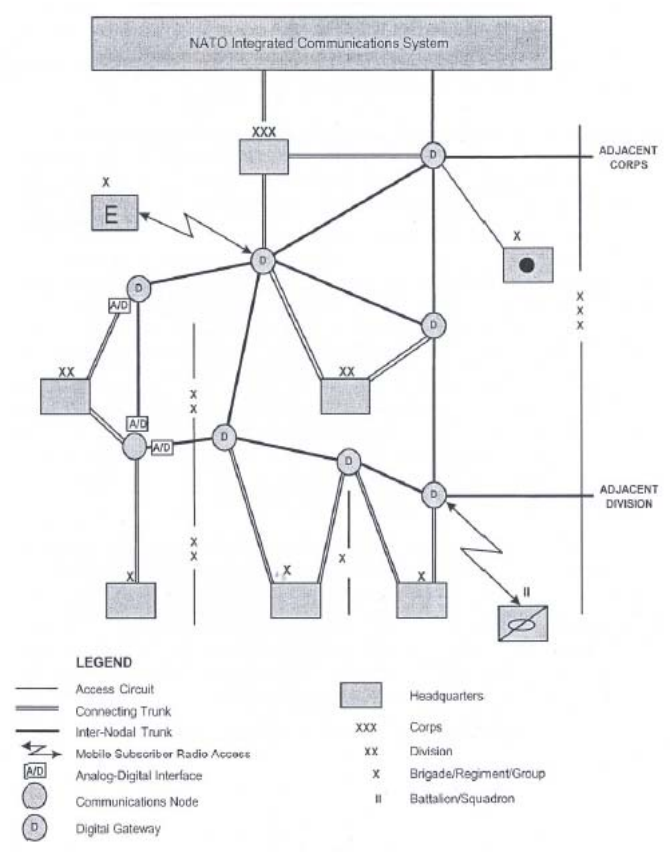

Fig. 3. Minimum scale of tactical communication system connectivity

C. *Tactical Radio System*

Tactical radio system is in every case the key component of the tactical level communication, which is able to secure different services. Up-to-date software radios enable transmission of information between soldiers, vehicles, command posts and weapon control systems via open or closed network, with restricted bandwidth. Beyond voice-based communication provided also by general radios, it secures different means of communication (sending pictures, GPS data, tactical sms, tactical chat, etc.). Nowadays Kongsberg MH300 radios are standard for VHF band, the different (PRC) devices of Harris radio-family for HF band and also types of Rohde & Schwarz radios. Radio-connection is capable to transmit information with the utilization of the benefits of wire free communication. On tactical level, the modern radios are the fundaments with its wide-ranging multipurpose communication capabilities. These equipment are ensure connectivity between different level of command posts (CP), different type of users (soldier, armored vehicle) in ground and air (GAG radios, UAV connections). This part of the communication and information system is the most relevant in the field (mobile) communication system. The Fig. 4 shows the dimensions of the modern JTRS [6].

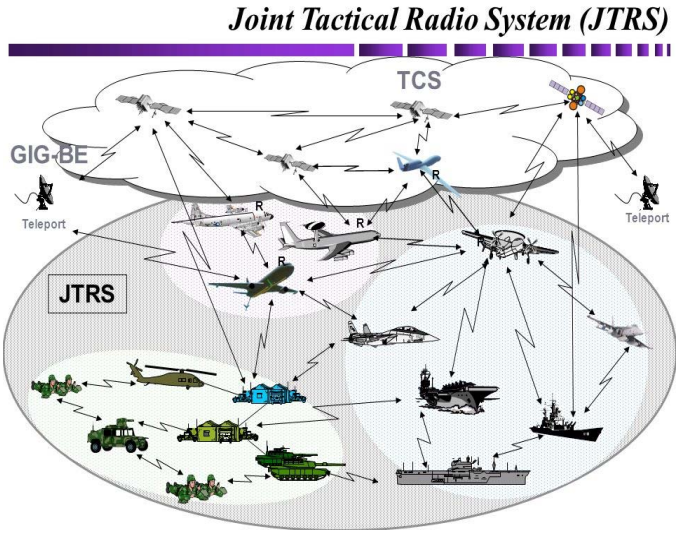

Fig. 4. Dimension of JTRS

In summary the common utilization of all three networks together secures complex support of info-communication, which enables the services to be ready in every case. A good example to this is the info-communication support of mission tasks and the expanded border-security tasks caused by the migration. Only difference (from info-communication side) is the variety of utilized assets and networks, which is verification for the importance of modularity! Thus the field network on its own cannot, or only at basic level be regarded as a complex support system. A complex system involves beyond those mentioned above, also GSM networks, Satellite connections and Tetra network as well.

III. Trends of Network Development

Development of subsystem elements within field command system is a primary objective in the creation of an up-to-date system. Basic step, and inevitable to meet all the command and

operational acquirements is the multifaceted and complex task of defining the signals operational requirements.

In accordance with the development of field radio and information system already realized (digital tactical radios, command complexes, signal venter assets) it is inevitable that the future system elements have to be able to cooperate and be interoperable. Thus such tools and technologies have to meet the national and allied requirements and regulations, and the recent and future (expected) operational conditions.

An important feature is that the field system is only meeting the requirements if it is able to secure beyond the field services also the stationary telecommunication and information services necessary for operational success as described above. During the planning of the realization, compatibility and interoperability thus cooperation with already accessible state-of-the-art field equipment; stationary information system; allied information systems and public info-communication systems are most important aspects,

It is important that the system in its whole complexity has to meet the national and NATO standards; the future plans of NATO system technology development; allied regulations (policy, directives, STANAG); the expectations of NNEC (NATO Network Enable Capability). *"The formal definition of NNEC says that it is "the Alliance's cognitive and technical ability to federate the various components of the operational environment, from the strategic level down to the tactical levels, through a Networking and Information Infrastructure (NII)"" [7].*

The Fig. 5. present the components of the NNEC, which is one of the main capability for the cooperation. [7].

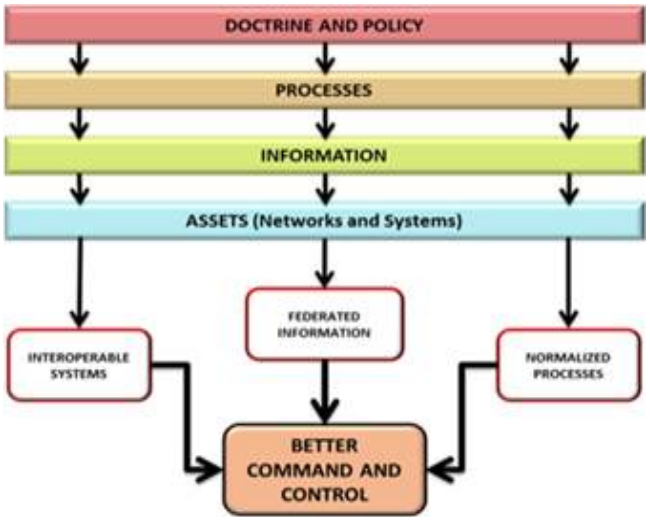

Fig. 5. The components of NNEC

"For disparate systems to work together, NATO has traditionally focused on interoperability. NNEC picks up from there and through the four components […] identifies requirements, guidelines and solutions that will allow effective sharing of information and services supported by standards, joining instructions, data management practices, adequate information assurance and commensurate policies. NNEC looks at the ability to exchange information and, more importantly, at the ability to exploit that information, addressing the non-technical aspects of interoperability in the process" [7].

Beyond these modularity; support of expeditionary capacity; network based running; expandability; and the support of different information systems have to be basic features. Several of the essential principles and requirements are held in the allied documentation, like JP 6-0 Joint Communication System, or AJP-6 Allied Joint Doctrine for Communication and Information Systems, which are to be aware of during planning and development. Such other requirements are: information assurance, flexibility, spectrum management, data security, timeliness, innovation, adaptation, survivability, protection, and many others [8]; [9].

Beyond the general requirements as above, other features have to be counted with when shaping each sub-system. Primary aspects of analyzation in the recent phase of research and development are the possibilities and abilities within shaping the communication systems between the standard HIK/G signal center and the command posts of different (ops, tac) levels, and within the command posts themselves.

The HIK/G field communication center deployed and ran on command posts possesses all capabilities which are required to meet operational needs, while it is able to integrate the connecting command posts and stations into a signals and information network.

During the definition of required signals and information abilities of each command post, general operational necessities and the personal conditions of C2 have to be held in sight. Firstly a complex field command post securing the C2 towards the troops has to be realized. On the long term quick (re)deployability, small physical volume, which is still able to secure the work of the personnel are also key features.

On a long term it would be practical to create a field command post built up from containers, which can secure the complex action of C2. Such a post from „container modules" (in a volume sufficiently built for each level) can assure quick deployability (deploying, connecting) and after physically built up it can be ready to use. From signals and information aspect it is an important benefit that the containers can be cabled as the desks and terminals are prescribed beforehand, physical LAN networks can already be deployed, places for the possibly beforehand built in active and passive elements can be described, and also inevitable electric support and acclimatization can be secured. Within the command post Wi-Fi network access would be easier to maintain, but recent regulations permit such, thus cable remains the only option for that. To deploy such in a tent, and casually with not regular or not prescribed workplaces to connect into a network, can be time consuming and elaborate. Thus on tactical and operational level the solution with containers would be more sufficient from signals and information aspect. Within the command post on lesser distances copper wire connection is more practical, which can support the LAN network needs of the command post sufficiently. Using containers would be a more sufficient answer also from the view of information protection, since due to the metal body it provides electromagnetic coverage which

makes the building of inner protected networks with copper wire possible. This solution also makes modularity and quick deployability possible which can be a key element during crisis response operations and also while catastrophe relief tasks. During the establishment of the signals and information system of the command post, the communication and information systems already in use and planned are to be aware of, which can be: voice based communication network (VoIP; ISDN; VTC); compatibility towards Legacy systems (E&M; CB; LB; G3 fax; etc.); internet/intranet; blue force tracking (C2; BFTS); reconnaissance/surveillance systems and databases; aerial and ground fire control systems; other sensors (UAV; meteorology; etc.); picturing devices; ciphering and data protection; other subsystems and networks [10].

With the recent principles and lines of NATO development in sight, to establish IP based communication is more the suggested way to go instead of ISDN systems (WAN side), which can only partially meet recent requirements. Realization of short-distance inner connections can be done by the utilization of Powerline technology, which enables deployment to be even easier, while long-distance (wire) connection is only suggested with optic cable, which can cover long distances and high data speed.

The main technical parts of the mobile CIS center are shown on Fig. 6. This unit is separated six different type of functional subsystem. These are responsible for the different connectivity and functional switching roles [10].

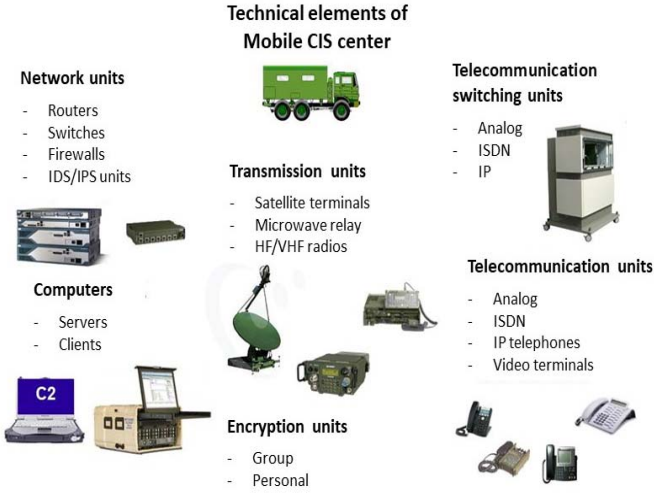

Fig. 6. Mobile communication center (HIK/G)

Beyond the above it is also important that it can secure the classification, integrity, and disposability of information during the transmission, and also maintenance, in respect to the vulnerability of the information, the regulations and the NATO directives.

IV. Conclusion

To realize command under field conditions a modern, state-of-the-art C2 system, ready to meet the requirements, and to work sufficient under special conditions is inevitable. The advancing development of information systems is affecting the C2 systems in use with Hungarian Defense Forces as well. The info-communication system providing support needs constant development which has to involve also the command post as elements of it.

The lined up primary features and acquirements enable it to meet national and allied requirements, and provide greater possibility of cooperation with allied military organizations and other national defence organizations as well. All these are inevitable in the fulfilling of different tasks. Furthermore other important condition, to meet the requirements of NNEC, network operations and all the battlefield digitalization and different type of interoperability. The battle command system (BCS) is one of the most integrated system, which integrate all the information in one system, and all the participants reach the necessary information. The significant advantages of the BCS are the follows:

- All the information are in one system.
- Faster MDMP (Military Decision Making Process).
- Easier planning.
- Situational Awareness (SA).
- Integrated system.
- Map-based display (system)

The BCS is consist of the following elements:

- Battle Command Sustainment Support System
- Integrated Meteorological Environmental Terrain System
- Air and Missile Defense Planning and Control System
- Maneuver Control System
- Digital Topographic Support System
- Tactical Airspace Integration System
- Advanced Field Artillery Tactical Data System
- Blue Force Tracker

The modernized and interoperable info-communication system has to support all the commanding chain in different level and different type of tasks with in-time-information in full spectrum of operation. The Fig. 7. presents the levels and components of network based operation supported by modernized communication network [11].

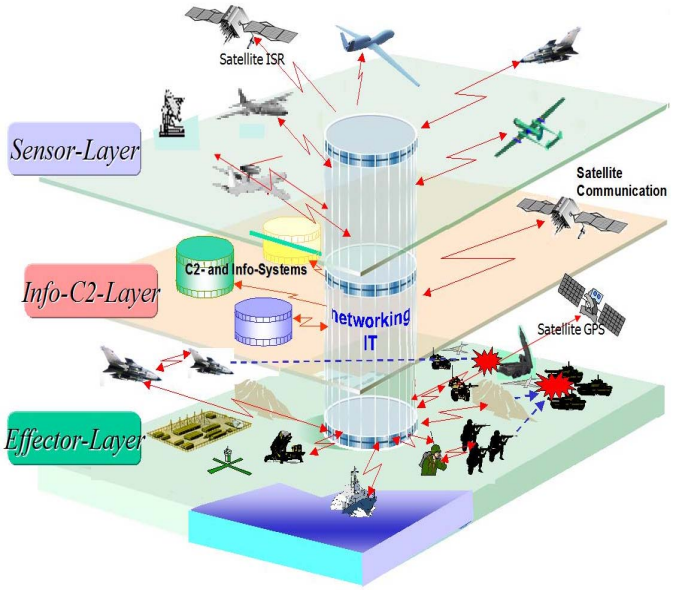

Fig. 7. Network Based Operation

In summary the system has to support leadership on all level between the given organisations; from sub-unit through combat vehicle to the soldier; the fulfilling of task at recon and artillery sub-units; and also the training of staff can be a key element which can be realized with the use of the system.

REFERENCES

[1] G. Szem, "Network-based command-control systems, as possible sources for future military history research," in Hadmérnök vol. 1, pp.210-222. March 2016.

[2] G. Szem, "A hálózatalapú vezetési-irányítási rendszerek mint a hadtörténeti kutatás lehetséges jövőbeli forrásai," in Bolyai szemle, vol. 2, pp.77-91. June 2015.

[3] K. Fekete, "The Main Technical characteristics of the insular Telecommunication network for Purpose of Government of the Hungarian Defense Forces," in Bolyai szemle, vol. 1, pp.70-77. March 2015.

[4] J. Rajki, "A Magyar Honvédség Stacioner Híradó hálózatának modernizálási lehetősége a jelenlegi infrastruktúra továbbfejlesztésével," MSc thesis, NUPS p. 9. 2014.

[5] The minimum scale of connectivity for communication and information systems for NATO land forces (STANAG 5048), NATO MAS, p. 50. February 2000.

[6] R. Gearhart, "Presentation", [21st Annual symposium. Defense Acguistion University Virginia, USA 2003], http://slideplayer.com/slide/8027561/ (downloaded, 04.15.2017.)

[7] NATO Network Enabled Capability (NNEC) http://www.act.nato.int/nnec (downloaded, 04.15.2017.)

[8] Joint Chiefs of Staff, Joint Communications System (JP 6-0), June 2015.

[9] Allied Joint Doctrine for Communication and Information Systems (Ajp-6), NATO NSA, April 2011.

[10] A. Szabó, "Az ip telefon rendszerek katonai alkalmazhatóság-vizsgálatának lehetőségei," in Hadmérnök vol. 1, pp.195-209. March 2016.

[11] K. Benedict, "Enterprise Mobility, Netcentric Operations and Military Mobility," August 2014.
http://mobileenterprisestrategies.blogspot.hu/2011/08/enterprise-mobility-netcentric.html (downloaded: 04.19.2017)