Prof. Mariusz Frączek
e-mail: mfraczek@ap.edu.pl
ORCID: 0000-0002-2216-8053
Pomeranian Academy in Słupsk
DOI: 10.26410/SF_2/21/7

TECHNICAL PROTECTION OF CYBERSPACE LAND FORCE – GENERAL ASSUMPTIONS

ABSTRACT

The publication presents the basic issues related to the technical protection of cyberspace, as well as its impact on the functioning of telecommunication networks troops. The author pointed out the issues of growing challenges, adopted and its impacts in existing areas. Also shows the overall impact of cyberspace on the security of information. An important theme of discussion is to identify the main challenges of protecting cyberspace that can implemented on command posts in the Land Forces. They have to not only increase the security of information, but also all soldiers.

Keywords

information security, information and communications, cyberspace, security

Introduction

The military communication system is a part of the state telecommunication system designed to ensure the transmission of information for the needs of troops in times of peace, crisis and war. Its architecture is formed by forces and consists of communication and information technology, developed in a manner corresponding to the organization of command and the nature of operations.

The communication system should ensure continuous, covert, timely and reliable exchange of information. It enables efficient command of troops and directing of means of warfare[1]. Thanks to it military command functions and communication with non-military forces is ensured. Military communication system consists of three subsystems: command, information exchange (communication network) and supply.

The criterion of exploited means of communication causes that, in classical terms, the communication system consists of four elements:

1. Telecommunications networks.
2. Computer networks.
3. Military field mail.
4. Signaling network.

The dynamic development of information technology and the phenomenon of convergence of services means that the first two elements have formed a single ICT network[2]. Currently it is the foundation of the ability of the army to information exchange. It enables the provision of communication services for commanders and soldiers. Communication system has a broader meaning than communication network, which in colloquial terms are often equated with each other.

The Military communication network is a network of forces and consists of communication deployed in a specific area and working according to a plan to exchange information and direct combat encounter[3].

In the XXI century there has been an increased interest in modern solutions in the field of communications. The Land Forces have defined new expectations and challenges in this area for the operation of command posts, communications networks and the ability to operate automated systems of command and direction of means of warfare. It was agreed that used military, automated command systems will have the ability to share data with other systems of own troops and systems of other NATO countries through standardization of data exchange. The target state is to reach ability to secure transmition of information in electronic form by all military systems and ICT networks, as well as having access to them by all authorized soldiers.

Cybersecurity of Land Forces

Security – the meaning of this term in terms of organization and operation of a given information and communication network cannot be defined unequivocal. It has an interdisciplinary meaning and

[1] *Regulamin działań wojsk lądowych,* DWLąd 115/2008, Warszawa 2008, pkt. 14027.

[2] M. Frączek, *Wieloaspektowość kształtowania bezpieczeństwa sieci teleinformatycznej wojsk lądowych*, Warszawa AON 2015, p. 31.

[3] J. Mazurkiewicz, *Leksykon łączności wojskowej*, AON, Warszawa 1996, p. 176.

this is a result of its various interpretations available in the literature[4].

It is impossible to unequivocal indicate which of them best reflects the essence of the presented issue. According to the author, ICT network security should be identified with ensuring, in the indicated place and time, a state which means no risk of information loss or losses in the elements of the ICT network. Therefore, it is a state obtained as a result of an organized (organizational and technical) protection against possible threats, expressed in the ratio of the possessed potential intended to ensure information protection and the possibility of using forces and means appropriately to the scale of threats[5].

The challenge facing ground troops is determining the importance of cybersecurity to ensure their ability to accomplish their stated tasks. Similarly, as in the case of the ICT network, the author has a number of doubts related to the interpretation of the term cyberspace contained both in legal acts, as well as the literature on the subject[6]. According to the Polish law it is also defined heterogeneously and it is rather impossible to work out an unambiguous definition accepted by all expert environments. From the perspective of the tasks set for the army, one could base the service activities only on the provisions of the Act of 30 August 2011[7]. Cyberspace is as the space of production and exchange of information created by information and communication systems. The Act allows for the use of all available resources and means to defend it, not excluding military action. In addition, it allows the possibility of imposing martial law on the territory of our country resulting from an attack in cyberspace and the implementation of all possible measures to defend our own computer networks[8].

According to the author, one of the most important documents in which the term cyberspace was defined is the Doctrine of Cyber Security of the

[4] *Regulamin Działań Wojsk Lądowych,* DWLąd Wewn. 115/2008, Warszawa 2008, *Słownik definicji. Encyklopedia wiedzy komputerowej, Warszawa 2006*, Biblioteczka Komputer Świat No. 3/03 (23), p. 213. Liderman K., *Podręcznik administratora bezpieczeństwa teleinformatycznego*, Warszawa 2003, p. 18. Liderman K., *Analiza ryzyka i ochrona informacji w systemach komputerowych*, PWN, Warszawa 2008, p. 11-12. *Encyklopedia Nauki i techniki*, Prószyński i spółka, Warszawa 2002, tom I, p. 139.

[5] M. Frączek, *Wieloaspektowość kształtowania bezpieczeństwa sieci teleinformatycznej wojsk lądowych*, Warszawa AON 2015, p.79.

[6] *Dictionary of the English Language, Fourth Edition copyright* ©2000 by Houghton Mifflin Company. Updated in 2009. Published by Houghton Mifflin Company, *Random House Kernerman Webster's College Dictionary*, © 2010 K Dictionaries Ltd. Copyright 2005, 1997, 1991 by Random House, Inc., *Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016*, Ministerstwo Spraw Wewnętrznych i Administracji, Warszawa 2010, p.6, Ustawa z dnia 17 lutego 2005 roku *„O informatyzacji działalności podmiotów realizujących zadania publiczne"*, Art. 3, pkt. 3., M. Frączek, *Wieloaspektowość kształtowania bezpieczeństwa sieci teleinformatycznej wojsk lądowych*, Warszawa AON 2015, p. 149-151.

[7] Ustawa z dnia 30 sierpnia 2011 roku *O zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw.*

[8] M. Frączek, *Wieloaspektowość kształtowania bezpieczeństwa sieci teleinformatycznej wojsk lądowych*, Warszawa AON 2015, p. 150.

Republic of Poland[9], which indicates strategic directions for ensuring the desired level of security in cyberspace and further defines it as the space of processing and exchange of information created by information and communication systems, together with the interconnections between them and relations with users[10].

It is worth noting that the aforementioned Doctrine... attempted to reconcile different environments and to develop a compromise on the functioning of the armed forces in cyberspace, among other things. Hence, another concept called cyber security environment appeared. It is defined as the totality of conditions for the functioning of a given entity in cyberspace[11]. Thus, the meaning of the term cyberspace is permanently evolving. It should be noted the ongoing heated discussions among people of science on the genesis and meaning of the term cyberspace and various, not always uniform interpretations of it, because the precise characterization of cyberspace is difficult, which is due to various reasons.

One of the most important institutions tasked with protecting the state from external aggression is the military. Therefore, protection against cyberwarfare has been reflected in Polish law with respect to the functioning of the entire armed forces, thus including the land forces.

Cyberwarfare is also referred to as cyberattack. Generally, it is the use of an ICT network to conduct offensive operations with the help of dedicated software. The essential features of cyber warfare, are:

a. gaining information superiority,
b. invisibility of the adversary,
c. the area of operation is cyberspace, so perhaps the entire world;
d. time is the critical factor.

The author believes that, security in cyberspace should be equated with ensuring a state that means no risk of losing information important to the user or organization as a result of the application of security undertakings adequate to the scale of threats[12].

War in cyberspace is conducted by commanders at all levels and levels of command as part of combat operations. It is not a colloquially understood war of computer scientists against each other – between IT specialists (good/ blue) and IT specialists (bad/ red).

In computer networks of telecommunication operators, it is erroneously assumed that only information in electronic form exposed to cybercrime[13], cyberterrorism[14] and hacktivism should be protected.

[9] *Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej* z dnia 22 stycznia 2015 roku, wyd. BBN, wyd. Warszawa 2015. *Przesłanie Prezydenta Rzeczypospolitej Polskiej.*

[10] Ibidem.

[11] *Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej* z dnia 22 stycznia 2015 roku, wyd. BBN, wyd. Warszawa 2015. *Przesłanie Prezydenta Rzeczypospolitej Polskiej*, Wprowadzenie, p. 5.

[12] M. Frączek, *Wieloaspektowość kształtowania bezpieczeństwa sieci teleinformatycznej wojsk lądowych*, Warszawa AON 2015, p. 152.

[13] A. Bógdal-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003, p. 325.

[14] D. E. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, Wydawnictwa Naukowo-Techniczne, Warszawa 2002, T. Jemioła, J. Kisielnicki, K. Rajchel, *Cyberterroryzm – nowe wyzwania XXI wieku*, Wydział Wydawnictwa i Poligrafii Wyższej Szkoły Policji w Szczytnie, Warszawa 2009 r.

The Land Forces ICT network primarily addresses cyber threats that affect its security. These include:

a. network operations,
b. electronic spectrum operations,
c. radio-electronic warfare,
d. network operations using computers.

The author's empirical research indicates that the goal of operations in cyberspace, is to achieve advantage and dominance on the electromagnetic battlefield. Protection of information, including classified information in accordance with the law On the protection of classified information of August 5, 2010, is only one of the many requirements necessary to meet.

Considerations and analyses of identified and potential threats to information security in the information and communication network of the land forces indicate the need to answer two questions:

1. Who or what should be protected?
2. How can cyberspace protection be ensured for units performing tasks at the tactical level?

Firstly, there are many differences between the information and communication network of the land forces and the services available to every Polish citizen. The same applies to the diversity of their threats. The military takes into account operations in the electromagnetic spectrum and the capabilities of the future opponent in the field of radio-electronic warfare. Modern resources of reconnaissance allow to effectively disrupt radio systems, but also to indicate the location of the development of command posts, which are the objects of air force and artillery attacks. The main conclusion – knowledge of threats and rules of information protection may be decisive for survival of soldiers.

Poland's participation in NATO means access to knowledge, joint cooperation and consideration of response to various scenarios of potential attacks in cyberspace domain. It is also important for one's own security to build defensive capabilities in the face of anticipated threats.

Secondly, it should be noted that this issue is very complex and requires the implementation of many organizational and technical projects. Thanks to them it is possible to increase the protection of cyberspace of fighting soldiers. It should also not be forgotten that the military increasingly often performs tasks other than in wartime – as part of crisis response operations (rescue and evacuation actions, assistance during disasters or natural disasters, but also the fight against terrorism) or peace support operations.

In the paper the author's attention focused mainly on the technical area of cybersecurity.

Technical measures for information security in cyberspace

A necessary condition for the operation of any military ICT network is to equip it with technical means to ensure the security of information transmission. Digital devices meet high requirements for the protection of transmitted data. At the same time, in order to improve security, as well as to minimize errors in operation or access to network resources, opportunities will be created to automatically record the work of users and to control the transmitted information.

The implemented procedures for security of information transmission, device identification and connections are strictly enforced. Sophisticated technical protection methods are used, barriers for unauthorized people are created, which should effectively protect all information transmitted in the ICT network. It is not easy and requires a lot of forces and resources.

The security level of information exchange should be appropriate to the category of the transmitted messages and always strive to protect against unauthorized disclosure. The author proposed that technical security measures for information exchange in an ICT network should be divided into four types:

1. Hardware protection of an ICT network (transmission security).
2. Electromagnetic protection of ICT network.
3. Software influence on information security in ICT network.
4. Cryptographic protection of data communication network.

Hardware protection of ICT network

Observations indicate that currently used technical equipment operating in the information and communication network of ground forces in a limited way provide the desired level of protection for exchanged messages. The biggest shortcomings relate to the protection of messages transmitted at the level of company – battalion. On the other hand, a positive phenomenon is that commanders recognize the needs for an increase in information security in the technical aspect. There are also implemented solutions (multipurpose transmission vehicles/ command vehicles/ mobile command posts), the equipment of which meets high requirements.

Factors affecting the hardware security of the ICT network are:

1. The impossibility of theft of classified equipment and the exclusion of the possibility of replacing it with other equipment without compromising security.
2. Maximum use of external input-output for a given device.
3. The source of funds operating in an ICT network is known.
4. Devices used in an ICT network should meet the requirements of immunity to interference and the ability to delete data that should not be disclosed.
5. Maintaining a constant power supply for the operation of devices transmitting information.
6. Transmission security protecting the transmitted information against eavesdropping, traffic analysis, etc.

ITC network security always entails considerable financial outlays for the protection of lines and devices located within and outside the protection zones. In the field conditions it was considered optimal to use fiber optic cables in the areas of deployment of command posts, which guarantee high security of information and prevent (without their physical damage) eavesdropping of transmitted messages.

Electromagnetic protection of the ICT network

All electronic equipment is a source of electromagnetic emissions and requires an appropriate level of protection. This contributes to an increase in the cost of ensuring the safety of devices emitting electromagnetic energy. This issue is less important when performing tasks in garrisons due to the number of means of communication used, their protection and the use of fixed ICT infrastructure. The second pole of consideration are mobile systems deployed in areas of military dislocation.

Applied technical means can always be a source of information for the enemy. The following deserve special attention: devices emitting electromagnetic waves – especially medium-power radio stations. The same applies to computer network and radio-cable network. Another challenge that is difficult to exclude are cell phones used by soldiers, devices with access to the global network (palmtop/ netbook/ laptop/ tablet), as well as phones for satellite communications.

Transmission of information may be best secured in military networks, but there may always be an irresponsible soldier using a social networking site, who thanks to one photo will betray the location of own troops. There are many examples of this both by Russian/Ukrainian soldiers during the Russia-Ukraine conflict and by US soldiers during their stay in Iraq and Afghanistan.

Electromagnetic protection of ICT network is provided by placing telecommunication devices, connections and lines in protective zones, which guarantee EEM security. Various devices and technologies are used, the detailed characteristics of which will be omitted.

Practical assurance of safety against electromagnetic emissions is realized by:

1. Shielding of computers, transmission equipment and their cabling and the use of shielding booths.
2. The introduction into military equipment of equipment with very low power and thus low revealing emissions.
3. Operation of radio means at minimum power.
4. Placing computer workstations in restricted access areas.
5. Improving knowledge of the potential adversary's radio-electronic reconnaissance capabilities.

Achieving 100% electromagnetic security of the ICT network is difficult, but it represents the development of technical means of communication and information technology guaranteeing low revealing emission, which should then go to the troops.

Influence of software on information security in ICT networks

Software enables devices to operate using established management mechanisms and the sequence of individual tasks execution, as well as ensures information security. Conducted analyses allowed to conclude that software used in information and communication network of Land Forces should enable[15]:

1. Information exchange between network users.
2. Control of access to information transmitted in computer networks (identification of oneself and strangers) through logging of verified persons and access passwords dedicated to them.
3. Establishing barriers (mechanisms) preventing the introduction of viruses or other infected software – which can have permanent consequences in the form of network malfunctions.
4. Changing access codes (passwords) by authorized persons – remote control of the networks.
5. Meeting imposed security standards (the barrier above which access to the software does not occur) and at the same time allowing to work on it in the scope of its modernization, control, or work reports.
6. Full monitoring of information exchanged in a computer network, including determination of time of message transmission, addressees, urgency category, manner of message reception and whether it was an authorized recipient (by whom and when).

The software used in the Land Forces ICT network is less vulnerable to a variety of threats. This is due to the separation of military networks from the global network. Increased security of information exchange in ICT networks and minimization (exclusion) of a large number of errors during their operation is always associated with the use of proven software.

Cryptographic protection of the ICT network

Cryptography is the art of converting a written text, understandable to all into an encrypted text understandable only to insiders, who know the cipher[16]. Cryptography is a science that deals with the confidentiality of transmitted information. This term should also be understood as the art of securing messages[17]. Cryptography is also defined as an element of computer science that allows, through various methods, to secure the information created, transmitted or processed in digital form. It is a tool for securing services running online (transmission) or off-line (electronic mail), in a purely software, hardware or mixed[18] way.

Cryptographic protection is the application of methods and measures to secure information by encrypting it and using cryptographic mechanisms that guarantee the integrity and authentication of entities or information. In the land forces, it is used when transferring information outside controlled access zones. Data exchange always takes place in accordance with applicable laws. It should guarantee the following services:

[15] M. Frączek, *Wieloaspektowość kształtowania bezpieczeństwa sieci teleinformatycznej wojsk lądowych*, Warszawa AON 2015, p. 194.

[16] M. Szymczak (red. naukowa), *Słownik języka…*, wyd. cyt., tom I, p. 1063.

[17] B. Schneider, *Kryptografia dla praktyków*, WNT, Warszawa 1995, p. 19.

[18] A. Urbanek, *Ilustrowany leksykon teleinformatyka*, IDG, Warszawa 2001, p. 122.

a. confidentiality-Defines the extent to which data cannot be accessed or disclosed to unauthorized persons, entities, or processes;
b. integrity- protection against unauthorized modification of data;
c. authentication – verification of the declared identity of the subject;
d. nonrepudiation – the inability of one of the entities involved in the data exchange to deny its participation in all or part of the exchange.

The Land Forces troops use a variety of cryptographic means. The operation of special devices is aimed at ensuring the security of transmitted information at the highest level and they are the most guarded devices of communication and information technology elements of the network.

Summary

The growth of threats to information forces the constant search for and use of new, hard-to-break ways to protect it. Designed and used security system should protect against all threats, including those related to the fifth combat environment, which is cyberspace. Omitting or overprotecting always has a negative impact on information security. This is due to poor protection or difficult to avoid improper implementation of developed procedures.

Technical protection, as one of three important elements, should effectively ensure the security of information transfer. At the same time it should be noted that the deeper the awareness of the necessity to ensure information protection by people having access to it and the mutual co-operation of all its users, the better the security of information transfer can be. Observing the accepted rules, procedures and thus the established level of ensuring protection must not be treated as a necessary evil, but as a result of the necessity of such behavior accepted by everyone. The possibility of loss, interception, substitution or modification of transmitted messages must be limited, so that the accepted principles of its protection are not revealed.

The essential function of the communications system is to ensure continuity of information transmission for the command process. This can be achieved as a result of development and operation of modern communication networks, which will always and under any terrain and weather conditions have the ability to transmit messages. A positive trend of development is aiming at transformation of the current structure of military ICT network in the direction indicated in the assumptions of network-centric battlefield (NCW – Network Nentric Warfare/ NNEC – NATO Network Enabled Capacity). However, it should be kept in mind that it will require time and high costs of modernization or replacement of equipment.

The analysis of existing capabilities to ensure the security of technical protection of information and military in cyberspace indicates the following final conclusions:

1. The weakest element of the security system is man, because the most depends on him (use of information/ desire for profit/ pursuit of power/ system design

or committing crimes related to breaking into information resources).

2. Technological progress causes the development of ways to secure ICT networks and improve the means of acquiring information.
3. It is always necessary to strive for an optimal system ensuring technical security by combining the capabilities of various means.
4. Costs incurred for information transmission security should result in protecting messages according to the hierarchy of their importance.
5. The use of network monitoring system should ensure efficient detection of threats and network vulnerabilities.
6. Designing, organizing and implementing new devices should result in creating a secure working environment.
7. The problem of ensuring information and communication network security occupies much wider area of consideration than just virtual domain or technical means in general.
8. Execution of tasks by land forces (ICT network security) in the area of cyberspace is guaranteed by the interaction of all three factors. Organizational security and physical security author deliberately omitted in the study.
9. Currently ground forces are looking for and adapting new solutions and the latest information technologies. This process requires time to meet additional expectations related to information protection, which are defined in NATO and European Union documents.

To conclude, problems raised in this publication are only a prelude to proper research conducted in the widely understood area of cyberspace. The explicit character of the publication makes it necessary to present this area in general terms.

Bibliography

Bógdal-Brzezińska A., Gawrycki M.F, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003.

Denning D. E., *Wojna informacyjna i bezpieczeństwo informacji*, Wydawnictwa Naukowo-Techniczne, Warszawa 2002.

Dictionary of the English Language, Fourth Edition copyright ©2000 by Houghton Mifflin Company. Updated in 2009. Published by Houghton Mifflin Company.

Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej z dnia 22 stycznia 2015 roku, BBN, wyd. Warszawa 2015.

Encyklopedia Nauki i techniki, Prószyński i spółka, Warszawa 2002, tom I.

Encyklopedia wiedzy komputerowej, 2006, Biblioteczka Komputer Świat nr 3/03 (23).

Frączek M., *Wieloaspektowość kształtowania bezpieczeństwa sieci teleinformatycznej wojsk lądowych*, Warszawa AON 2015.

Jemioła T., Kisielnicki J., Rajchel K., *Cyberterroryzm – nowe wyzwania XXI wieku*, Wydział Wydawnictwa i Poligrafii Wyższej Szkoły Policji w Szczytnie, Warszawa 2009 r.

Liderman K., *Analiza ryzyka i ochrona informacji w systemach komputerowych*, PWN, Warszawa 2008.

Liderman K., *Podręcznik administratora bezpieczeństwa teleinformatycznego*, Warszawa 2003.

Mazurkiewicz J., *Leksykon łączności wojskowej*, AON, Warszawa 1996.

Random House Kernerman Webster's College Dictionary, © 2010 K Dictionaries Ltd. Copyright 2005, 1997, 1991 by Random House, Inc.

Regulamin Działań Wojsk Lądowych, DWLąd Wewn. 115/2008, Warszawa 2008.

Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016, Ministerstwo Spraw Wewnętrznych i Administracji, Warszawa 2010.

Ustawa *o ochronie informacji niejawnych* z dnia 5 sierpnia 2010 roku, Dz. U.10.18.1228.

Schneider B., *Kryptografia dla praktyków*, WNT, Warszawa 1995.

Szymczak M., (red. naukowa), *Słownik języka polskiego*, PWN, Warszawa 1993

Urbanek A., *Ilustrowany leksykon teleinformatyka*, IDG, Warszawa 2001.

Ustawa z dnia 17 lutego 2005 roku „*O informatyzacji działalności podmiotów realizujących zadania publiczne*".

Ustawa „*O świadczeniu usług drogą elektroniczną*" z dnia 18 lipca 2002 r.

Ustawa z dnia 30 sierpnia 2011 r. „*O zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw*".

About the Autor

Mariusz Frączek, retired officer of the Polish Army. Specialist in the field of technical security problems. He is interested in the issues of state security, military security, crisis management and cooperation of security systems.