Zeszyty Naukowe
Wyższej Szkoły Bankowej w Poznaniu
2018, t. 83, nr 6
DOI: 10.26349/zn.wsb.w.poznaniu.0083.05

Bartosz Biernacik

War Studies University
Military Studies Faculty
orcid.org/0000-0002-6797-6951
e-mail: b.biernacik@akademia.mil.pl
tel. +48 261 813 009

The Fifth Dimension of War – Cyberspace. How to Secure This Area: The Approach of Selected States and International Organizations to Cybersecurity

Abstract. Cyberspace is a fifth dimension of war. As the Internet grows the cyber activity is growing as well. Nowadays it is used for political and economic reasons as a pressure tool on countries. Therefore to secure the cyberspace is a growing issue. It has become important due to the more and more frequent examples of activity in cyberspace. The growing activity is unfortunately focused on cyber-terrorism, cyber-espionage, cyber hacktivist and more. To make it more complicated cyberspace is the place of almost full anonymity and it is hard to proof the guilty of the exact group or person. That is why international organizations like NATO, ENISA, and whole countries are building its abilities to act in cyberspace. Some of them are willing to act only to protect themselves but other are officially declaring also offensive activities. This article is a presentation of current trends in cyberspace in some of the biggest players in it.

Keywords: cyberspace, cyber operations, cyber-hacktivist, cyber-terrorism, cyber-espionage, Internet of Things

1. Introduction

One of the most important issue taken last year during the Warsaw Summit of NATO in July 2016 was to define cyberspace officially as the fifth dimension of war. That is why one of the most important issue of the cyberspace has become its security. Cybersecurity has become the most important issue for last few years for the security specialists as a result of growing popularity of the Internet. Nowadays we do not talk about Internet anymore – now we are facing new, bigger, better and more sophisticated version – Internet of Things (IoT). Growing number of items

connected with each other gives opportunity for the groups of people that wants to destabilize the situation in some places. Those places can be – group of people, social networks, cities or even countries.

This is the problem of growing importance of cyberspace that must be protected by specialists against that kind of activities.

Cybersecurity problems had found respond in plenty of international organizations as well as countries in a specialized organizations dealing with cybersecurity issues on a daily basis. This article will provide basic information about them as well as some of the most important for Europe security organizations.

But to start with the cybersecurity issue we have to understand the cyberspace at all. So what cyberspace is?

Cyberspace – it is a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers [JP 3-12].

Another definition say that cyberspace is: The space in which computer transactions occur, particularly transactions between different computers. We say that images and text on the Internet exist in cyberspace, for example. The term is also often used in conjunction with virtual reality, designating the imaginary place where virtual objects exist. For example, if a computer produces a picture of a building that allows the architect to "walk" through and see what a design would look like, the building is said to exist in cyberspace [The American Heritage New Dictionary of Cultural Literacy 2005].

Cyberspace [ˈsaɪbəˌspeɪs] noun 1. all of the data stored in a large computer or network represented as a three-dimensional model through which a virtual-reality user can move [Collins English Dictionary 2012] (Table 1).

No matter which definition of cyberspace we will take under consideration three things are in all of them – data stored in computers and communication between them by the network. Therefore we have to concentrate on those two things when we think about the cybersecurity.

Let's have a look how the international organizations deals with the cybersecurity.

2. European Network and Information Security Agency (ENISA)

ENISA as a civilian organization is responsible to protect civilian part of cyberspace of all the member countries of European Union (EU).

ENISA is a Centre of Network and Information Security Expertise for the EU, its Member States, the private sector and Europe's citizens. ENISA works

Table 1. Definition of Cyberspace in selected countries

Country / organization	Definition of Cyberspace term	Source of definition
Belgium	Translation: Cyberspace is the global environment for the interconnection of information and communication systems. Cyberspace is wider than the computer world and also contains computer networks, computer systems, digital media and digital data, whether physical or virtual.	Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America – 2014
Czech Republic	The cyber space is a very specific environment that has no geographic borders and in which the distance between the source of threat and the potential target becomes relative. Its asymmetric nature makes it possible for state as well as non-state actors to harm the Czech Republic´s strategic and important interests without using any conventional means.	Security Strategy of the Czech Republic – 2015
Hungary	Cyberspace means the combined phenomenon of globally interconnected, decentralized and ever-growing electronic information systems as well as the societal and economic processes appearing in and through these systems in the form of data and information.	Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America – 2013
Belgium	Translation: Cyberspace is the global environment for the interconnection of information and communication systems. Cyberspace is wider than the computer world and also contains computer networks, computer systems, digital media and digital data, whether physical or virtual.	Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America – 2014
Czech Republic	The cyber space is a very specific environment that has no geographic borders and in which the distance between the source of threat and the potential target becomes relative. Its asymmetric nature makes it possible for state as well as non-state actors to harm the Czech Republic´s strategic and important interests without using any conventional means.	Security Strategy of the Czech Republic – 2015
Hungary	Cyberspace means the combined phenomenon of globally interconnected, decentralized and ever-growing electronic information systems as well as the societal and economic processes appearing in and through these systems in the form of data and information.	Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America – 2013
Italy	Cyberspace is a man-made domain essentially composed of ICT nodes and networks, hosting and processing an ever-increasing wealth of data of strategic importance for States, firms, and citizens alike, and for all political, social and economic decision-makers.	Compilation of Existing Cybersecurity and Information Security Related Defintions, Open Technology Institute New America – 2013

Country / organization	Definition of Cyberspace term	Source of definition
India	Cyberspace is a complex environment consisting of interactions between people, software, and services, supported by worldwide distribution of information and communication technology (ICT) devices and networks.	Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America – 2013
International Organization for Standardization	The complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form.	Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America – 2012
Japan	Cyberspace, a global domain comprised of information systems, telecommunications networks and others, provides a foundation for social, economic, military and other activities.	Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America – 2013
Kenya	The notional environment in which communication over computer networks occurs.	Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America – 2014
Latvia	Cyber space is an interactive environment that includes users, networks, computing technology, software, processes, information in transit or storage, applications, services, and systems that can be connected directly or indirectly to the Internet, telecommunications and computer networks. Cyber space has no physical borders.	Source: Cyber Security Strategy of Latvia 2014-2018 – 2014
Lithuania	Cyberspace is a global space which has no national boundaries, hence, the rapid spread of threats across cyberspace	Source: Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America – 2011
Montenegro	National Security Strategy	Source: Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America – 2007
New Zeland	The global network of interdependent information technology infrastructures, telecommunications networks and computer processing systems in which online communication takes place.	Source: Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America – 2011
Poland	A space of processing and exchanging information created by the ICT systems, together with links between them and the relations with users.	Source: Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America – 2013
Romania	Translation: Cyberspace is characterized by the absence of borders, dynamism, and autonomy, creating opportunities to develop both knowledge-based information society and risks to its operation.	Source: Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America – 2013

Russia	Translation: A sphere of activity within the information space, formed by a set of communication channels of the internet and other telecommunications networks, the technological infrastructure to ensure their functioning, and any form human activity on them (individual, organizational, state).	Source: Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America – 2014
Spain	Cyberspace, the name given to the global and dynamic domain composed of the infrastructures of information technology – including the Internet – networks and information and telecommunications systems, has blurred borders, involving their users in an unprecedented globalization that provides new opportunities but also entails new challenges, risks and threats.	Source: Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America – 2013
Switzerland	The state, the private sector and society make use of information and communication infrastructure and access to cyberspace (Internet, mobile networks and applications, e-business, e-government, computer-based control programmes).	Source: Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America – 2012
Turkey	The environment which consists of information systems that span across the world including the networks that interconnect these systems.	Source: Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America – 2013
The Netherlands	For the purposes of this strategy, „cyberspace" is understood to cover all entities that are or may potentially be connected digitally. The domain includes permanent connections as well as temporary or local connections, and in all cases relates in some way to the data (source code, information, etc) present in this domain.	Source: Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America – 2012
UN/Lebanon	Cyberspace, as a network using the Transmission Control Protocol/Internet Protocol (TCP/IP) communications protocol, has shown itself to be a fragile and insecure environment which has allowed criminal groups to attack and, on occasion, destroy it, because priority has been given to commercial and marketing objectives.	Source: Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America – 2007
UK	An informal word first thought to have been used by novelist William Gibson to refer to the total data on all computers on all the networks in the world. The word has passed into common use as a way of referring to any large collection of network-accessible computer-based data.	Source: Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America – 2008
US	The notional environment in which communication over computer networks occurs	Compilation of Existing Cybersecurity and Information Security Related Defintions, Open Technology Institute New America – 2008
South Africa	Cyberspace means a physical and non-physical terrain created by and/or composed of some or all of the following; computers, computer systems, networks, and their computer programs, computer data, content data, traffic data, and users.	Security Related Defintions, Open Technology Institute New America – 2012

Source: own elaboration based on https://ccdcoe.org/cyber-definitions.html [access: 1.08.2018].

Figure 1. ENISA Strategy 2016-2020

Source: www.enisa.europa.eu/publications#c5=2007&c5=2017&c5=false&c2=publicationDate&reversed=on&b_start=0 [access: 1.08.2018].

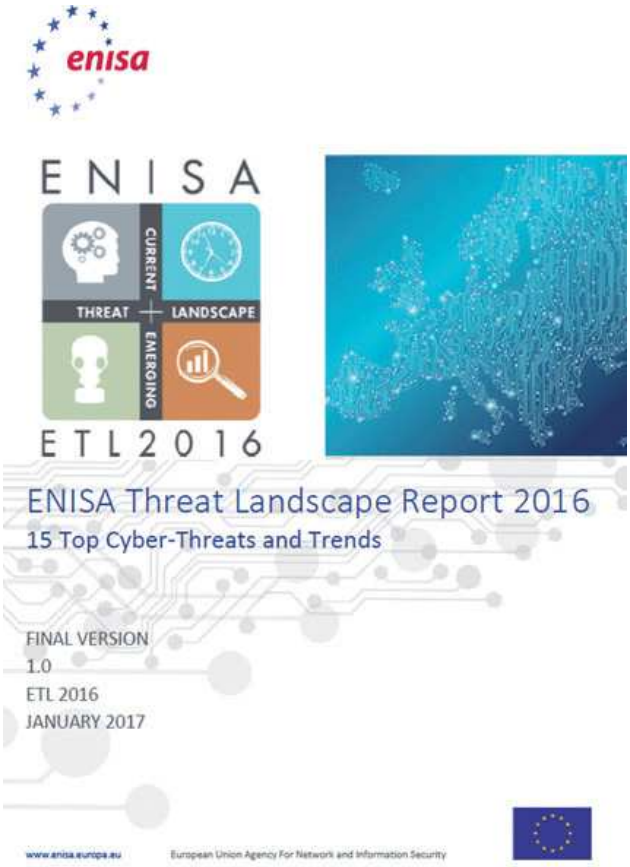

Figure 2. ENISA Annual report – ENISA Threat Landscape Report 2016.

Source: www.enisa.europa.eu/publications#c5=2007&c5=2017&c5=false&c2=publicationDate&reversed=on&b_start=0 [access: 1.08.2018].

with these groups to develop advice and recommendations on good practice in information security. It assists EU Member States in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks.

ENISA seeks to enhance existing expertise in EU Member States by supporting the development of cross-border communities committed to improving network and information security throughout the EU.

Agency produces plenty of documents that are guidelines for civilian national agencies. Its library consist of hundreds' of books defining cyber security issues. It has its own strategy defining planning activity of ENISA. Latest was defined for years 2016-2020 (Fig. 1).

Agency produces also annual report (Fig. 2) that contain main problems of cyber security and list of the biggest and the most important treats for each year (Fig. 3).

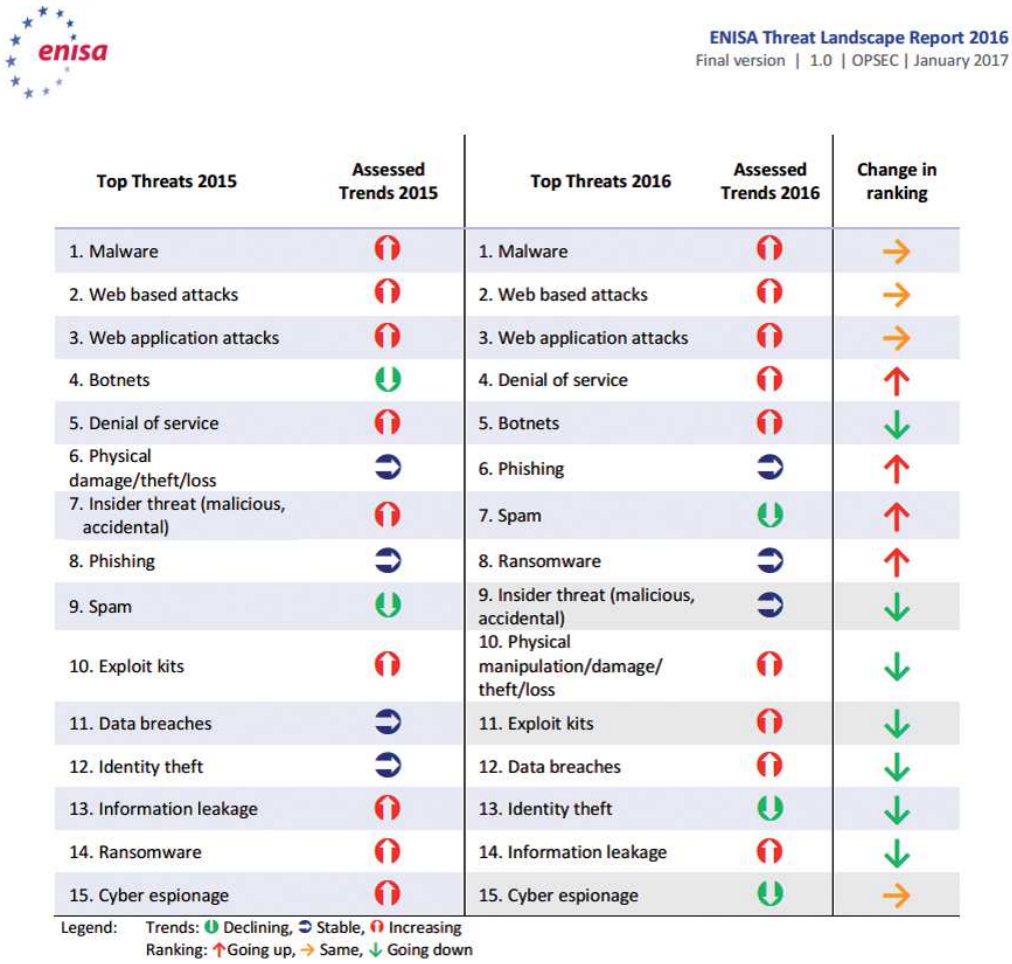

Figure 3. Top 15 threats in 2015 and 2016 from ENISA Threat Landscape Report 2016.

Source: www.enisa.europa.eu/publications#c5=2007&c5=2017&c5=false&c2=publicationDate&reversed=on&b_start=0 [access: 1.08.2018].

ENISA is also responsible to conduct the exercise for the specialists. Latest – Cyber Europe 2016: was the pan-European exercise to protect EU Infrastructures against coordinated cyber-attack (Fig. 4).

The exercise is a flagship activity organized every two years. Realistic scenario is prepared for thousands of experts from all 28 EU Member States, Switzerland and Norway which are facing it this challenge.

Cyber Europe 2016 (CE2016) was the largest and most comprehensive EU cyber-security exercise to date. This large-scale distributed technical and operational exercise started in April 2016, offering the opportunity for cybersecurity professionals across Europe to analyze complex, innovative and realistic cybersecurity incidents. On 13th and 14th of October ICT and IT security industry experts from more than 300 organizations, including but not limited to: national and governmental cybersecurity agencies, ministries, EU institutions as well as internet and cloud service providers and cybersecurity software and service providers were called upon to mitigate the apex of this six-month long cyber crisis, to ensure business continuity and, ultimately, to safeguard the European Digital Single Market[1].

Figure 4. ENISA – Cyber Europe.

Source: www.enisa.europa.eu/news/enisa-news/cyber-europe-2016 [access: 1.08.2018].

Cyber Europe 2016 painted a very dark scenario, inspired by events such as the blackout in an European Country over Christmas period and the dependence on technologies manufactured outside the jurisdiction of the European Union. It also features the Internet of Things, drones, cloud computing, innovative exfiltration vectors, mobile malware, ransomware, etc. The exercise was focused on political and economic policies closely related to cybersecurity. This also took into account new processes and cooperation mechanisms contained in the Ne-

[1] www.enisa.europa.eu/news/enisa-news/cyber-europe-2016 [access: 1.08.2018].

twork and Information Security (NIS) Directive. For the first time, a full scenario had been developed with actors, media coverage, simulated companies and social media, bringing in the public affairs dimension associated with cyber crises, so as to increase realism to a level never seen before in cybersecurity exercises.

The Cyber Europe motto was expression: stronger together. Cooperation at all levels is key to the successful mitigation of major, borderless cyber incidents.

ENISA as an EU cybersecurity agency plays a key role in EU cyber preparedness. The NIS Directive[2] is a major step forward the EU's abilities to deal with large cross border incidents that can lead to such crises. The CSIRT Network established by the Directive, along with work done so far for the EU Cyber Europe cycle, are key in providing decision makers with an overview of the situation and ultimately to respond to such complex threats.

ENISA, the European Commission and the Member States are investing in strengthening of an EU-wide cybersecurity crisis cooperation. The future of cyber crisis management in Europe – currently planned by the European Commission, concerns the drafting of a cyber crisis cooperation plan and the development of a cyber crisis management platform. ENISA's exercises provide a unique opportunity to test new developments, prepare for the future and develop further the sense of cooperation in the EU.

2.1. NATO Cooperative Cyber Defense Centre of Excellence and NCI Agency

NATO (Fig. 5) as a military organization is responsible to protect military part of cyberspace of all the member countries. Of course it is not possible to do such a thing by one organization. Therefore in NATO there is an organization named NATO Cooperative Cyber Defense Centre of Excellence (NATO CCD COE) which is the International Organization of the Military. It was accredited by the North Atlantic Council of NATO on 28 October 2008. The center is located in Tallinn, Estonia at the Estonian Battalion stationed Communications.

CCD COE's mission is to improve the capacity and potential of defense cooperation and information sharing among NATO members and their partners in the field of cyber defense through education, research, development, collecting experiences and consultations.

The aim of the CCD COE is to become the main source of knowledge and specialist skills in the area of cyber defense through the collection, production and dissemination of knowledge in this field among NATO members and their partners.

[2] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive [access: 1.08.2018].

Figure 5. NATO Headquarters in Brussel

Source: www.nato.int/cps/en/natohq/organisation.htm [access: 1.08.2018]..

Cyber defense center in Tallinn is one of 21 accredited Centres of Excellence (COES), training for high-tech aspects of NATO operations.

COEs generally specialize in one functional area and act as subject-matter experts in their field. They distribute their in-depth knowledge through training, conferences, seminars, concepts, doctrine, lessons learned and papers.

In addition to giving NATO and partner country leaders and units the opportunity to augment their education and training, COEs also help the Alliance to expand interoperability, increase capabilities, aid in the development of doctrine and standards, conduct analyses, evaluate lessons learned and experiment in order to test and verify concepts.

COEs work alongside the Alliance even though NATO does not directly fund them and they are not part of the NATO Command Structure. They are nationally or multi-nationally funded and are part of a supporting network, encouraging internal and external information exchange to the benefit of the Alliance. The overall responsibility for COE coordination and utilisation within NATO lies with Allied Command Transformation (ACT), in coordination with the Supreme Allied Commander Europe (SACEUR).

Currently, there are 24 COEs. They all have NATO accreditation. The working language of COEs is generally English.

The main tasks of the Centre are:

– improving interoperability within the framework of the Network Enabled Capability (NATO NNEC),

– developing doctrines and teaching methods and the development of concepts and their validation,

Figure 6. NCI Agency structure

Source: www.nato.int/cps/en/natohq/organisation.htm [access: 1.08.2018].

– increasing the security of information and education of cyber defense, raising awareness and training in the field of cyber-security,

– providing support for cybersecurity during the experiments / military exercises (including those conducted on the spot),

– analysis of the legal aspects of cyber defense.

The center has also other obligations, which include:

– contribution to the development of practice standards and cyber defense with NATO PfP candidates NATO and non-NATO countries,

– contribution to the development of security policy NATO cyber defense, to define the scope and responsibilities of the military in cyberspace,

– conducting cyber defense training, information campaigns, workshops and courses,

– developing and carrying out defense exercises in cyberspace.

Another organization that is responsible for sustain cybersecurity within NATO is NATO Communications and Information Agency (NCI Agency)[3]. In the-

[3] The NATO Communications and Information (NCI) Agency was established on 1 July 2012 as a result of the merger of the NATO Consultation, Command and Control Agency (NC3A), the NATO ACCS Management Agency (NACMA), the NATO Communication and Information Sys-

ir structure (Fig. 6) you may find Cyber Security Cell that is responsible for secure the cyberspace of NATO Headquarters and networks.

The NATO Communications and Information Agency (NCI Agency) Cyber Security (CS) Service Line (SL) is responsible for planning and executing all life cycle management activities for cyber security. The Cyber Security Service Line provides specialist cyber security-related services covering the spectrum of scientific, technical, acquisition, operations, maintenance, and sustainment support, throughout the life cycle of NATO information communications and technology, enabling secure conduct of the Alliance's operations and business in the NNEC environment and in the context of NATO's Command, Control, Communications, Computers, Intelligence, Surveillance (C4ISR). The Service Line provides cyber security services to NCI Agency customers and users, as well as to all other elements of the Agency, including all Service Lines, Programme Offices, CIS Support Units/Elements, and the Agency Ops Centre. Cyber Security is responsible for providing the broad spectrum of services in the following specialist security areas: CIS Security, Cyber Defence, Information Assurance, Computer Security & Communications Security. In executing its responsibilities, the CS SL provides support to the development and implementation of cyber security-related policy, strategy, and provides lifecycle security risk management services for all NATO ICT. Cyber Security leads in the development of new capabilities and innovation in cyber security. Cyber Security incorporates the NATO Computer Incident Response Capability (NCIRC) Technical Centre, providing specialist services to prevent, detect, respond to and recover from cyber security incidents.[4]

As an example it is good to mention here that the NCI Agency's Team (Cyber Security and Education & Training Service Lines and the Legal Office) provided an important contribution to the success of the biggest Cyber Defence exercise NATO has ever held. The Cyber Coalition 2017 (CC17) exercise was conducted 28-30 November, with more than 900 participants from 29 nations and the EU. The aim of the exercise was to train collaboration and information sharing between NATO, nations and partners in response to cyber threats. The Exercise Objectives were set by NATO's Military Committee.

To summarize activity of this organization we may say that this is not an organization that protect physically the cyberspace of NATO countries. It tries to secure its own networks as a NATO organization. It is an organization that cooperate with all of the member countries as well as PfP countries to build better standards and protection of the cyberspace. The responsibility of the active protection is still

---

tems Services Agency (NCSA), the ALTBMD Programme Office and elements of NATO HQ ICTM. Source: www.ncia.nato.int/About/Pages/About-the-NCI-Agency.aspx [access: 1.08.2018].

[4] www.ncia.nato.int/Our-Work/Pages/Cyber-Security.aspx [access: 1.08.2018].

put on the country level, therefore NATO countries must strongly cooperate and work to build up cyber protection abilities, to avoid cyber-attacks.

2.2. United States Cyber Command – US CYBERCOM

One of the most advanced in cybersecurity countries are United States if America. They have two main organizations dealing with cyber – NSA (National Security Agency) (Fig. 7) and US CYBERCOM (United States Cyber Command) (Fig. 8).

Figure 7. NSA emblem

Source: www.cyberdefence24.pl/eksperci-przed-komisja-ds-sil-zbrojnych-nsa-trzeba-oddzielic-od-uscybercom [access: 1.08.2018].

The National Security Agency (NSA) is a national-level intelligence agency of the United States Department of Defense, under the authority of the Director of National Intelligence. The NSA is responsible for global monitoring, collection, and processing of information and data for foreign intelligence and counterintelligence purposes, specializing in a discipline known as signals intelligence (SIGINT). The NSA is also tasked with the protection of U.S. communications networks and information systems [About NSA: Mission 2014; Ellen Nakashima 2008] The NSA relies on a variety of measures to accomplish its mission, the majority of which are clandestine[5].

As part of the National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD 54), signed on January 8, 2008, by President Bush, the NSA became the lead agency to monitor and protect all of the federal government's computer networks from cyber-terrorism.[Ellen Nakashima, 2008].

[5] www.enisa.europa.eu/publications#c5=2007&c5=2017&c5=false&c2=publicationDate&reversed=on&b_start=0 [access: 1.08.2018].

Figure 8. US CYBERCOM emblem

Source: www.wired.com/images_blogs/dangerroom/2010/06/2010-05-14-USCYBERCOM_Logo_Cropped-660x660.jpg [access: 1.08.2018].

The second organization, dealing with cyberspace is one of the largest Cybernetic Army in the world, the Army of the United States, which has, consisting of:

– Army Cyber Command/2nd Army,

– The Network Technology Command/9th Signal Command Army (NETCOM),

– The 1st Information Operations Command Land (1st IO Command),

– The U.S. Intelligence and Security Command (INSCOM).

US CYBERCOM combines the full spectrum of operations the cyber US Department of Defense, plans, coordinates, integrates, synchronizes and implements the defense and protection of information networks Department of Defense (DoD), coordinates the operations of the DoD to support military missions by management networks for the themselves. Prepares, manages and runs the entire range of military operations in cyberspace. Command uses currently owned power and resources by building structures of cooperation and synchronizing effects of combat operations to combat threats in cyberspace.

USCYBERCOM combines the full spectrum of operations the cyber US Department of Defense (DoD), plans, coordinates, integrates, synchronizes and implements the defense and protection of information networks DoD, coordinates the operations of the DoD to support military missions by management networks. Prepares, manages and runs the entire range of military operations in cyberspace.

Command uses currently owned power and resources by building structures of cooperation and synchronizing effects of combat operations to combat threats in cyberspace.

The Americans intend to Create a fully developed forces to act in cyberspace (up to 2018) – Cyber Mission Force (CMF).

CMF is planned to have 133 specialized teams of protection, which are the first line of defense of the state against any threats in the sphere of cyber hacktivists, relating both to the activities of third countries, companies and individuals.

It is estimated that the number of these forces CMF will eventually be 6,200 US military and civilian operators. The process of preparing and equipping the necessary hardware facilities began in 2013.

So far, the United States can boast of 3100 the operators of this type, coming from the four branches of the military.

They operate in the existing 58 teams.

Until recently determined role of CMF is a three element as a set of tasks related to security, first of all, the Department of Defense, secondly, in the broad sense of the United States and the activities carried out for the needs of the individual commands combat.

According to the plan:

– 13 teams is to focus the defense of the United States and used by the state of critical infrastructure, susceptible to all kinds of cyber threats,

– 68 teams are directly responsible for the protection of the Department of Defense and its networks, which are targeted by foreign and American hackers,

– 27 teams are responsible for offensive part, subordinated, every day, commanders of combat,

– 25 teams – facilities and support, especially in the field of analytics for these teams to be another.

US DoD in the doctrine of Joint Publication 3-12 (Fig. 9). Cyberspace Operations presented the principles of planning, preparation, conduct and evaluation of operations in cyberspace.

This document presents the operational activities in cyberspace at all levels of command and control. Defined concepts, task areas and identifies relationships and connections in the combined operations conducted with the use of elements in the fight cyberspace.

Another very important document for the US is the latest Cyber Strategy (Fig. 10) from April 2015 in which for the first time US officially confirm will of active offensive activities in cyberspace to protect America against the enemy.

The Department of Defense Cyber Strategy 2015 defines 5 main goals:

– build and maintain ready forces and capabilities to conduct cyberspace operations,

– defend the DoD information network, secure DoD data, and mitigate risks to DoD missions,

– be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyberattacks of significant consequence,

– build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages,

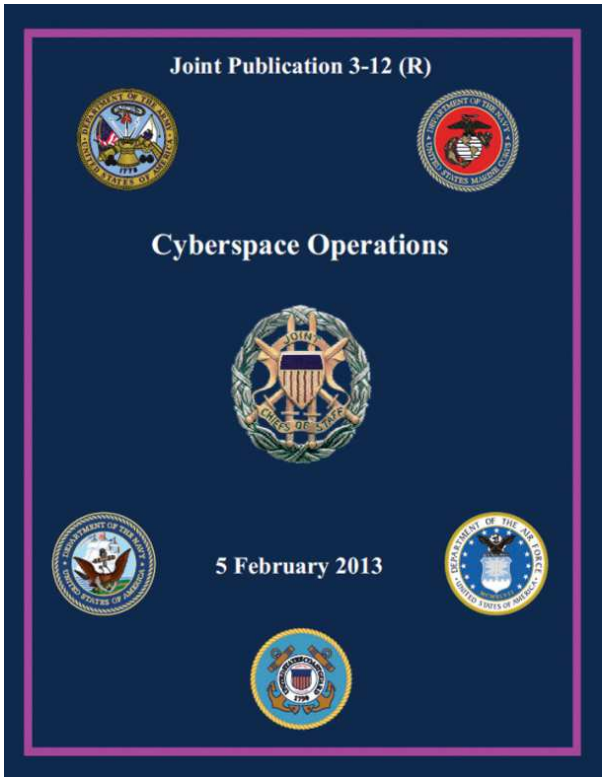

Figure 9. JP 3-12 (R), 5 February 2013

Source: JP 3-12 (R), Cyberspace Operations, https://fas.org/irp/doddir/dod/jp3_12.pdf [access: 1.08.2018].

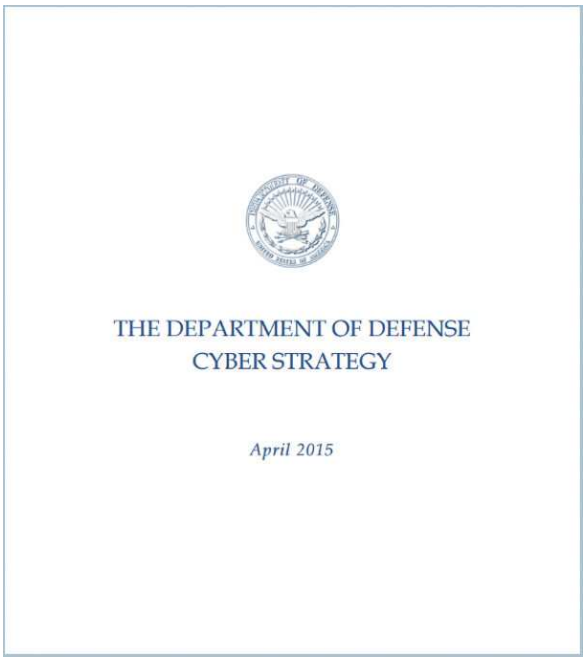

Figure 10. Cyber Strategy, April 2015

Source: Cyber Strategy, www.hsdl.org/?abstract&did=764848 [1.08.2018].

– build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability.

2.3. Germany National Cyber Defense Center and National Cyber Security Council

In Germany there are two main offices responsible for cybersecurity. Construction of the offices are similar to solutions made in Great Britain. One of them is National Cyber Defense Center (NCDC).

NCDC in Germany is operating under the Federal Ministry of Internal Affairs since 16th June 2011 with the task of creating better safety standards and procedures for defense in the area of cyberspace for both the private and the state sector.

Center serves as a common platform for the rapid exchange of information and coordination of activities against the security event information.

The mission of the Center for cyber defense in Germany is quick and comprehensive assessment of security incidents in order to develop recommendations and a coordinated response.

To achieve this goal, it organizes the collection and analysis of information about vulnerabilities in the products and results of the analysis of security incidents and attacks, as well as proposals for protective orders.

The second organization is planned to be created a National Cyber Security Council (NCSC) acting under the auspices of advisors for German Chancellor dedicated to the ICT matters, with the tasks of securing the flow of information between government, industry, safety authorities, telecommunication companies.

The main tasks of these entities is to collect information and data concerning Internet security and to provide decision-makers with expertise in the management of IT security.

In addition, it was decided to create a powerful cell counterintelligence dedicated exclusively fending off attacks on government servers. The Federal Intelligence Service (FIS in German: BND) conducts a large-scale recruitment of new intelligence officers. Instead, agents are looking for the best computer scientists who specialize in the field of security.

2.4. Great Britain Officer of Cyber Security and Cyber Security Operations Center

In 2010, Great Britain started to operate two cells involved in cyber security: Officer of Cyber Security (OCS), which conducts strategic consultancy in the field of cyber security for the UK government and is responsible for the creation and supervision of the government program for achieving strategic priorities of cyber security.

Cyber Security Operations Center (CSOC), which has the task of monitoring and ensuring cyber security and incident response directed against users and data communications networks in the UK, as well as advising and informing about the dangers of both in the sphere of business and the public.

Great Britain has also developed its own cyber security (Fig. 11).

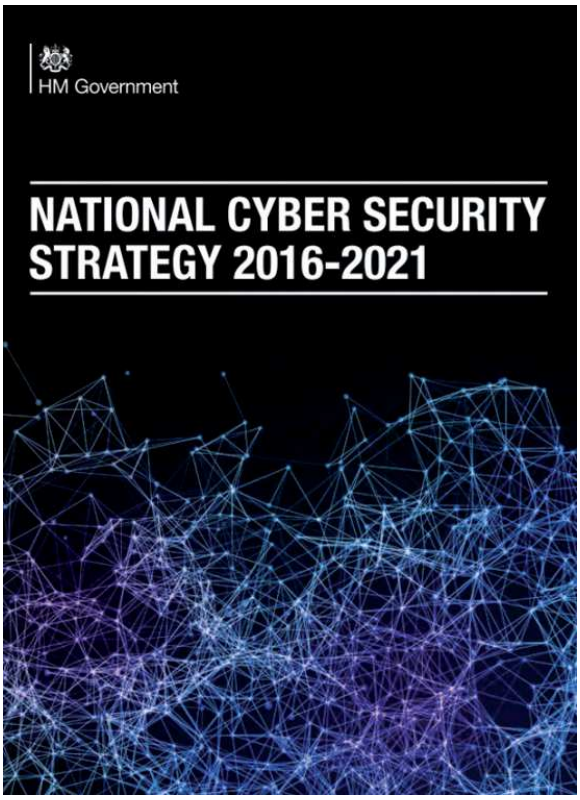

Figure 11. National Cyber Strategy 2016-2021

Source: National Cyber Strategy 2016-2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf [access: 1.08.2018].

2.5. China's Blue Fighter Army and Strategic Assistance Force

Another example of countries are the most active and aggressive China, which officially confirmed the creation of cyber troops May 25, 2011, They are part of the Chinese People's Army – Liberation.

The creation of so-called Blue Fighter Army spent probably about $ 1.5 million. The main activity of this elite unit is "defending the interests of government and business in cyberspace China."

Currently, the unit has been included in the structure of the Military Command Center in the Chinese province Guangdog the south of the country.

In addition, within the framework of the reform of the Chinese army, created a new unit to specialize, among others, in hostilities on the Internet and cyber espionage.

Strategic Assistance Force (SSF) are to ensure that the Chinese army will be able to make the Internet more efficient and more advanced offensive and reconnaissance.

It also has to protect the government against cyber-attacks. The unit consists of three parts. The first is the "soldiers – hackers" responsible for cyber-attacks and cyber defense. The second will deal with military operations in space, focusing on reconnaissance and satellite navigation. The third is to deal with the conduct of the war in the network. It also has to interfere with the operation of the devices radar and communication opponent. The unit also has the use of civilian technology: cloud computing, artificial intelligence and nanotechnology.

2.6. North Korea

North Korean regime has created a team of approx. 3000 cyber warriors whose task is to build a network of support for state authorities, and above all for Kim Jong-un, as well as spreading among Internet southern properly crafted propaganda.

It has to be done using the comments placed on South Korean websites. The North Korean cyber unit includes, among others 200 agents with writing online comments aimed at southern neighbor.

The purpose of propaganda is to demoralize the enemy and to help in the task they have stolen from the South Koreans virtual identity.

Propaganda is promoted by using hosted 140 sites in 19 countries.

North Korea educates its cyber specialists in elite schools in Pyongyang, and the most aptitude hackers are then directed to the 10-year training in the Military Academy Kim Il Sung and other universities.

Only in June 2013 Cyborg Soldier regime blocked 65 South Korean websites, stole the data of 2.5 million members of the ruling in the Seoul Grand National Party, 300 thousand military and 200 thousand site users belonging to the president of South Korea.

South Korean military intelligence claims that North Korea has recently doubled from three to six thousand numbers of their "cyber forces" – special formations dealing with hacker attacks.

The task of the "Office 121" as the name of this unit is to attack targets in South Korea. As for interfering with the functioning of the South Korean armed forces, the government's work, calling the "psychological shock", causing "physical and psychological paralysis" of the South (the information the Defence Ministry in Seoul).

Probably, the "121 Office" has for years been expanded by the North Korean military intelligence. They work there the most talented computer experts. From the information provided by defectors from North Korea that "Office 121" can plan the attack, including a telecommunications facilities and power network in South Korea.

In 2013, Seoul accused North Korea of hacker attacks on computer systems of South Korean banks and broadcasters.

At the end of November 2013 Sony Pictures was the victim of cyber-attack, which the FBI was derived from North Korea.

The attack was connected with plans to introduce released comedy "The Interview" about a fictional plot to kill North Korean leader Kim Jong-un.

Following the threats of hackers Sony Pictures canceled shows, but soon after changed its position and the film was to hundreds of American cinema, and has been in the United States available online for a fee and cable networks in the context of video on demand.

Pyongyang denies it was behind the attack.

2.7. Russian Federation

Russian Armed Forces had built their own digital shield to protect against cyber threats. The Russian Ministry of Defense planned to complete in 2017 the creation of a special body whose main task will be to protect critical facilities of the Russian armed forces from hackers.

In Russia for a long time, there are cell information security and combating organized cybercrime. The structure has a FSB (Federal Security Service), which is to fight cyber-terrorism in the channels public communications networks in the preparation of terrorist acts.

3. Conclusion

To summarize it should be mention again that nowadays we are living in the environment that is strongly connected with IT technologies and transformation of the Internet into Internet of Things is a fact. The fact is also that all of this is in the cyberspace which is growing issue for the whole Europe and most of the world.

The European ICT Industry is one of the most advanced in the world. Making the EU's single market fit for the digital age could contribute €415 billion per year to our economy and create hundreds of thousands of new jobs. The pervasiveness of high-speed connectivity and the richness and quality of online services in the European Union are among the best globally. Such advantages have considera-

bly increased the dependability of European citizens on ICT services. These two elements, quality of services and customer base, make this industry particularly appealing to global business. What if this important piece of the global economy becomes a target? Computer security attacks are increasingly used to perform industrial reconnaissance, lead disinformation campaigns, manipulate stock markets, leak sensitive information, tamper with customer data, sabotage critical infrastructures.

Problems of cybersecurity are growing nowadays and they will become the most important issue in near future. Future war fight will (rather already common war fight) are to be conducted in cyberspace. Cost of the operation in cyberspace is much lower than use of armed forces – and it is hard to prove who is guilty and who conducted the attack. Disruption in the economy of the attacked country is much bigger by using cyberspace rather than traditional forces.

Therefore we must as an European Countries try to do our best to improve our cybersecurity capabilities and prepare ourselves to conduct full spectrum of activities in cyberspace: defense ad well as offensive operations. Collaborative work of the countries as well as international organizations is (as we may think today) the best way to achieve success and avoid big cybersecurity violations. Near future may redefine our approach to this issue and we must be prepared to make huge and fast changes in order to be able to response fast and adequate to the possible danger from opponents side.

References

About NSA: Mission. National Security Agency, 14.09.2014.

Collins English Dictionary – Complete & Unabridged 2012 Digital Edition William Collins Sons & Co. 1979, 1986, Harper Collins Publishers 1998, 2000, 2003, 2005, 2006, 2007, 2009, 2012.

Cyber Strategy, www.hsdl.org/?abstract&did=764848 [access: 1.08.2018].

Ellen Nakashima (January 26, 2008). Bush Order Expands Network Monitoring: Executive Order 13470 – 2008 Amendments to Executive Order 12333, United States.

https://ccdcoe.org/cyber-definitions.html [access: 1.08.2018].

https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive [access: 1.08.2018].

Intelligence Agencies to Track Intrusions, *The Washington Post*, 9.02.2008.

Intelligence Activities, July 30, 2008, https://fas.org/irp/offdocs/eo/eo-13470.pdf [access: 1.08.2018].

JP 3-12 (R), Cyberspace Operations, https://fas.org/irp/doddir/dod/jp3_12.pdf [access: 1.08.2018].

National Cyber Strategy 2016-2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf [access: 1.08.2018].

Russia National Security Strategy, December 2015, www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf [access: 1.08.2018].

The American Heritage New Dictionary of Cultural Literacy, 2005, Boston, Mass.: Houghton Mifflin Company.

www.cyberdefence24.pl/eksperci-przed-komisja-ds-sil-zbrojnych-nsa-trzeba-oddzielic-od-uscybercom [access: 1.08.2018].
www.enisa.europa.eu [access: 1.08.2018].
www.enisa.europa.eu/news/enisa-news/cyber-europe-2016 [access: 1.08.2018].
www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa2019s-role-in-the-european-digital-single-market-dsm [access: 1.08.2018].
www.enisa.europa.eu/publications#c5=2007&c5=2017&c5=false&c2=publicationDate&reversed=on&b_start=0 [access: 1.08.2018].
www.wired.com/images_blogs/dangerroom/2010/06/2010-05-14-USCYBERCOM_Logo_Cropped-660x660.jpg [access: 1.08.2018].

Piąty wymiar wojny – cyberprzestrzeń. Jak zabezpieczyć ten obszar: podejście wybranych państw i organizacji międzynarodowych do cyberbezpieczeństwa

Streszczenie. Cyberprzestrzeń jest piątym wymiarem wojny. Wraz z rozwojem Internetu rośnie także aktywność w cyberprzestrzeni. Obecnie ten wymiar działań jest wykorzystywany ze względów politycznych i ekonomicznych jako narzędzie nacisku na państwa, dlatego zabezpieczanie cyberprzestrzeni staje się coraz większym problemem i coraz silniejszą potrzebą. Jest to ważne z uwagi na coraz więcej przykładów „zorganizowanej" działalności w cyberprzestrzeni, która koncentruje się głównie na cyberterroryzmie, cyberszpiegostwie i cyberatakach. Zabezpieczenie cyberprzestrzeni jest o tyle skomplikowane, że jest ona miejscem niemal pełnej anonimowości i trudno jest udowodnić (w przypadku działań specjalistów z tej dziedziny) winę konkretnej grupie lub osobie. Z tego powodu organizacje międzynarodowe, takie jak NATO, ENISA, a także całe państwa, przygotowują się do działania w cyberprzestrzeni. Niektóre z nich ograniczają się tylko do ochrony swoich zasobów w cyberprzestrzeni przed potencjalnymi intruzami, inne zaś oficjalnie deklarują, poza wspomnianą obroną, również działania prewencyjne w cyberprzestrzeni. Artykuł ten prezentuje aktualne trendy w cyberprzestrzeni u niektórych z „największych graczy" w tym obszarze.

Słowa kluczowe: cyberprzestrzeń, operacje cybernetyczne, cyberhaktywizm, cyberterroryzm, cyberszpiegostwo, Internet rzeczy