Scientific Journal of the Military University of Land Forces
ISSN: 2544-7122 (print), 2545-0719 (online)
2021, Volume 53, Number 2(200), Pages 245-255
DOI: 10.5604/01.3001.0014.9780

Original article

Cyberspace as a domain of operational activities and the resulting challenge

Piotr Hałys

Faculty of Mechanical Engineering, Wroclaw University of Science and Technology, Poland,
e-mail: p.halys@ron.mil.pl

INFORMATION

Article history:

Submited: 27 June 2019

Accepted: 24 July 2020

Published: 15 June 2021

ABSTRACT

The aim of the article is to inform the reader of contemporary threats to state security resulting from the progressive digitalization and automation of subsequent areas of life. This article is an attempt to answer the most important questions asked by the author, including: How should we think about the domain of cyberspace in its entirety – war, peace, and everything in between? How can the government and the private sector be on the same page when they encounter and must generate solutions to cyberspace threats?

KEYWORDS

safety, cyberspace, state security, information warfare

Introduction

In today's world, significant threats to the security of states do not have to be exclusively kinetic. The ongoing digitization and automation of subsequent areas of life means that more and more processes cannot take place without digital support. At the same time, the Internet of Things (IoT) concept is developing rapidly. Herein, the everyday devices that surround us become part of the cross-border information exchange system. What is more, every second, Internet users make hundreds of thousands of transactions on various social, entertainment and transaction websites. Indeed, the number of Internet users has exceeded 3 billion. In the US, for example, 88% of all Americans are online. In 2015, the number of emails sent exceeded 200 billion a day, while the number of Facebook users is 25% of the world's population. In Poland, almost 70% of the total population uses Google, and nearly 60% of users follow Facebook.

The incredibly fast world-wide development of the Internet and what results from this is presented by Cisco[1] in its latest report 'Visual Networking Index' (VNI). Here, Cisco predicts that by 2022, IP traffic on the network will be higher than for all the last 32 years combined, and in Poland, one person will have an average of 5.5 devices connected to the Internet. The

[1] Cisco Systems, Inc. – American IT company, the largest in the network industry in the world.

report also sees that by 2022, over 60% of the world's population will be Internet users. In addition, over 28 billion devices and connections will be online [1].

The report also shows data indicating that by 2022, 60% of the Polish population will be using the Internet, and from 2017 to 2022, IP traffic will increase in Poland three times (on average by 23% per year), reaching 2.7 exabytes data per month (980 petabytes in 2017). This is 4 times larger than in 2017 and 2 times larger than the fixed IP traffic in the same period of data transmission in Poland from mobile devices [1].

That is why the ability to defend own networks and tele information systems is so crucial, and the improvement of technologies used to conduct war in cyberspace has become a new challenge for the armed forces.

The term "cyberspace" was created for the needs of science fiction literature and popularized by William Gibson, who described cyberspace as an unimaginable complexity that is like "consensus hallucination experienced every day by billions of legitimate users in all countries" [2, p. 226]. Unfortunately, cyberspace is also where cybercrime runs rampant. According to the Symantec report, the losses resulting from the activities of cybercriminals in the world in 2011 amounted to 388 billion dollars, and 69 percent of all adult Internet users have been at least once (44% in 2011) victims of online crime. To a large extent, this is due to the fact that 41 percent of all users do not have current security software for computer systems [3, p. 126].

Cooperation in the fight against threats in cyberspace

Therefore, a key challenge faced by the world's largest economies is:

How can the government and the private sector be on the same page when it comes to cyber threats and their solutions?

In response to such threats, in 2017, the Polish government adopted the first cyber security strategy under the name "National framework for cybernetic security policy of the Republic of Poland for 2017-2022". The document defines four basic specific objectives:

1. Achieving the ability to coordinate actions at the national level aimed at preventing, detecting, combating and minimizing the effects of incidents violating the security of ICT (Information and Communication Systems) essential for the functioning of the state.
2. Strengthening the ability to counter cyberthreats.
3. Increasing national potential and competence in the field of security in cyberspace.
4. Building a strong international position of the Republic of Poland in the area of cybersecurity.

In August 2018, the first Polish law on the national cyber security system entered into force. The Act implements the Network and Information Security (NIS) Directive on measures ensuring a high common level of security of network and information systems in the territory of the European Union and determines the organization of the above system, tasks and bundles of entities creating the system and defines basic concepts, including the concept of cyber security as the resilience of Information Technology (IT) systems to all activities that violate the confidentiality, integrity, availability and authenticity of the processed data or related services offered by these information systems.

However, in order to meet today's threats in cyberspace, the joint effort of the private sector, government and science is needed, hence at present, in Poland, many national institutes

and universities actively carry out research projects within umbrella of the research work of the Ministry of National Defense, as part of projects at the National Center for Research and Development, as well as in international projects including in the European Defense Agency.

Poland is also involved in numerous initiatives in the area of training and exercises in the field of cyber security. Young people have the opportunity to learn and improve their skills during such events as the HackYeah competition at the end of last year in Warsaw, which for several days focused on the efforts of several hundred programmers to prove the security of current IT systems. The Ministry of National Defense and the Armed Forces of the Republic of Poland are interested in the best of them, which is why actions are taken that will interest and attract them to service.

In addition, the Ministry of National Defense launched a program in cooperation with the Lodz University of Technology, the Polish Armaments Group and Chełmoński High School in Łowicz. As part of the program in general secondary schools, classes with a cyber security profile will be created in smaller towns. "We want at least one partner class of the + Cyber. mil program with a class + cybersecurity profile to function in every province".

Moreover, the Ministry of National Defense announced the launch of the Military Secondary Technical High School at the Military University of Technology, increased admission limits for military studies and formed the Non-Commissioned Officer (NCO) School of Information Technology and Communications, while at the Military University of Technology (MUT) with foreign partners, it launched Master of Business (MBA) postgraduate studies in the field of cyber security.

The Polish science and industry sector has great potential in the field of proffering cyber security solutions, and the available instruments and financial solutions should soon make it more recognizable, allowing participation in the global supply chain of cybersecurity products as an innovative and dignified trust partner.

Though threats and devices change, cyber crime and cyber security threats do not change. The constant need to guard the security of state and of its citizens requires the work of exceptionally talented people, including IT specialists, mathematicians, and cryptologists. This is why the Ministry of National Defense supports all educational initiatives that mitigate the problem of IT insecurity. Hence, changes in the approach to cyberspace are also visible in increasing the number and competence of professional soldiers and activation, including implementing workshops on the use of the most effective technologies in the field of cyber security has begun. These include group work methods such as 'Design Thinking for Polish veterans' by the Kazimierz Pulaski Foundation and 'Veteran State Activities Outside the State Borders' in cooperation with International Business Machines Corporation (IBM), the latter having so far carried out such projects for veterans in the US and Great Britain.

It should be mentioned here that such programs are very popular, in the USA alone, in the last 8 years in cooperation with non-profit organizations such as 'Corporate America Supports You', IBM has enabled support for 33,000 veterans.

What is extremely important is the main resource, according to the Kosciuszko Institute [4], which has been developed in recent years and which can be used to build a national cybersecurity ecosystem. This is the cybersecurity specialist. Poland abounds in cybersecurity talents, which is confirmed by numerous rankings and "hackatons". Polish programmers and hackers win in almost all known IT competitions, from 'Locked Shields' (2014), through the cycle 'Capture the Flag' (2014) to the unofficial world championship programmers, namely 'Hello World Open' (2014) and 'Google Code Jam' (2012).

According to HackerRank, Polish developers are in third place, just after IT specialists from China and Russia. As for the Java programming language, Poland is at the top of the list [5]. What's more, Poland is second only to Singapore among the leading programming centers from the point of view of enterprises and investors [6], which in turn increases the demand for qualified ICT specialists within the domestic market. Yet, current estimates show that there are still 40,000 vacancies left in the Polish ICT sector, despite the fact that Polish universities are educating 30,000 new graduates of fields related to this industry each year [7].

States and organizations, as well as private entities make a huge effort to effectively anticipate and counteract potential threats in the digital world, but the pace of change means that we will probably not have sufficient capabilities to defend ourselves at any moment. Hence, the important role of cooperation, as this allows for multiplying potentials and reducing costs that would otherwise have to be incurred individually.

Bearing in mind that the total Internet traffic has seen rapid growth in the last two decades (Table 1), and information has become a major economic asset, conditioning social development, but also carrying important social, economic and cultural challenges for this development. The significance of this world cannot be underestimated.

Entrepreneurs, more than any other professional group, should be aware that we are entering the era of the digital revolution in which information has become a new currency. We are more and more dependent on the security of our data. According to the "Cyber Threat Central and Eastern Europe (CEE) Region 2018" survey conducted by the CYBERSEC HUB platform among representatives from Central and Eastern Europe, Polish companies spend almost three times the average spending on cybersecurity in the region [8]. The most frequently distinguished forms of ICT threats are:

– hacking,
– cybercrime,
– cyber terrorism,
– the use of cyberspace as the fifth theater of military operations [9] or the effects of uncontrolled use of the Internet in the social and psychological sphere [10].

Cybersecurity is currently at the top of the list of challenges companies face worldwide. The widespread digitalization of the business we are witnessing has led to a significant increase in the threat of cyberattacks over the past few years. In order to investigate the level of protection against this type of threats in the Central and Eastern European region, the CYBERSEC

Table 1. The Cisco VNI forecast: historical Internet context

Year	Global Internet Traffic
1992	100 GB per day
1997	100 GB per hour
2002	100 GB per second
2007	2,000 GB per second
2017	46,600 GB per second
2022	150,700 GB per second

Source: [1].

HUB platform in Kraków, in the period from March to April 2018, conducted the "Cyber Threat CEE Region 2018" survey. Taking part in this were 500 Central European SMEs from the Czech Republic, Poland, Romania, Hungary and Slovakia that employ from 1 to 249 people [8].

The research results indicated that as much as 65 percent of all enterprises from the CEE region do not have a data protection strategy for their clients. Among the countries in the region, the situation is best in Poland, where more than half of companies declare having had put in place this type of solution. At the other end of the spectrum, are Czech and Slovak companies, where the level reaches only 23 percent. The increase in the number of attacks, as well as new regulations at the European Union (EU) level, suggest that the growing perception of the severity of cyber threats will translate into the development of the market of cybersecurity products and services in the coming years. The relatively low-saturated CEE market can show much more dynamic growth than mature markets in Western European countries [8].

A holistic approach to threats in the cyberspace sphere

After establishing cyberspace as the domain of operational activities, another key question arises:

How should we think about the domain of cyberspace in its entirety – war, peace, and everything in between?

The development of the Cybersecurity Strategy of the Republic of Poland for the years 2017-2022 was an extremely important step in building the ability to protect Poland in cyberspace.

The inter-ministerial group responsible for developing the strategy included representatives of the Ministries of Digitization, National Defense, Internal Affairs and Administration, as well as the Internal Security Agency, the Government Security Center, the National Security Office and NASK. The main purpose of this document is to provide a high level of security for the public sector, private sector and citizens in the provision or use of key services and digital services. In particular, the Strategy indicates:

- objectives in the field of IT security,
- the main entities involved in the implementation of the ICT security strategy,
- a management framework to achieve the objectives of the national strategy in the field of ICT security,
- the need for prevention and response in relation to incidents and restoration,
- the normal state disrupted by the incident, including principles of cooperation between the public and private sectors,
- approach to risk assessment,
- directions of approach to education, information and training programs regarding cyber security,
- activities related to research and development plans in the field of IT security,
- approach to international cooperation in the field of cyber security.

In building new capabilities, the development of formal and legal documents should be based on the experience of our US ally, which in 2011 recognized cyberspace as an operational sphere of war and announced a reaction to attacks in cyberspace, as well as to all other threats. This resulted in the creation of a body command dedicated to these activities

– US CyberCommand. Recent years have seen rapid changes related to cybersecurity in Poland, as a result of reforms and transformations in the key international structures to which Poland belongs, such as the North Atlantic Treaty Organization and the European Union.

Attacks in cyberspace are characterized by many common features. These include:

- asymmetry, understood as the disproportion between the forces and means that should be used to carry out an effective attack at any given moment, and the outlays and resources that should be used constantly to ensure the highest possible level of security,
- cross-border – the ability to carry out activities in another country is not related to having physical presence on its territory,
- speed – the fastest and the easiest to use method for carrying out large-scale criminal, intelligence, military or even political activities (like misinformation),
- a relatively large ease to hide the identity of the perpetrator,
- the ability to use the weakest points in the security system, and each chain is as strong as its weakest link.

Each member of NATO, also at the national level, must realize from the obvious consequences of considering cyberspace as the next operational domain, that it is necessary to mention here, above all, the need to build the ability to control, to recognize, as well as to hold the ability to act in an offensive way in cyberspace.

In August 2018, the first Polish law on the national cyber security system entered into force. The Act implements the NIS Directive on measures ensuring a high common level of security of network and information systems in the territory of the Union, and determines the organization of the above system, tasks and bundles of entities creating the system. Moreover, it defines basic concepts, including the concept of cyber security as the resilience of IT systems to all activities that violate the confidentiality, integrity, availability and authenticity of the processed data or related services offered by these information systems. The Act establishes new institutions: the Government Plenipotentiary for Cybersecurity (dealing with the coordination of cybersecurity activities in the Republic of Poland) and the College for Cybersecurity (advisory body at the government level).

The Act also defines the tasks of the Minister of National Defense related with the need to ensure the capabilities of the Polish Armed Forces to conduct military operations in cyberspace and to develop skills through the organization of training and exercises and training. As a consequence of the Act, a Response Team was established in the Ministry of National Defense on Computer Incidents of the Ministry of National Defense – CSIRT MON, whose tasks include monitoring and reacting to threats and incidents reported by entities subordinate to or supervised by the Minister of National Defense. Cybersecurity is, therefore, one of the priorities of the areas of activity for the Ministry of National Defense.

When we talk about cybersecurity, we naturally think about the technical-operational aspect of the issue – possible threats, specific incidents and actions taken by authorized state entities to counteract them. Activities in cyberspace are an inherent element of currently undertaken military operations or operations. It should be mentioned that during the NATO summit in Warsaw, cyberspace was considered the domain of operational activities. And this unambiguous declaration of NATO members raises many challenges and puts a lot of questions in front of every NATO member, as well as NATO as a collective, including – starting with the most fundamental:

– how to understand Article 5 of the Washington Treaty – cyberspace is a domain that has no boundaries, so how to adopt common criteria for assessing an attack on an alliance state committed in the cyber domain? This problem does not exist in traditional operational domains like land, sea and airspace where boundaries are clearly outlined,
– how to respond to an attack in cyberspace made as an alliance member?
– should we use all available forces or should the answer be limited to activities in cyberspace?
– what are the rules of using force in cyberspace (RoE – rules of engagement)?

However, since we have recognized cyberspace as another operational domain, I mean that there is no difference between traditional, kinetic understanding of threats, and their equivalent in cyberspace – it is therefore necessary to build/develop in this area, abilities that will be used to ensure the security of the Alliance and its members. The consequence of this approach is:

– firstly, the need for Member States to undertake independent actions (capacity development, building structures, training), as well as to develop joint initiatives within the Alliance (the ability to defend resources),
– and secondly, the need to undertake a difficult but necessary debate on offensive capabilities as an inseparable element of collective defense.

Following this line of thinking, after recognizing cyberspace as the domain of operational activities, there is the need to recognize that all subsequent NATO activities are a further consequence of the accepted commitments. It should be mentioned here, among others, the creation of a NATO plan for designating cyberspace as an operational domain (including the establishment of a Cyber Operations Center), for building defensive and offensive capabilities, and for training in and exercising cyberspace defense.

Together with our allies we have to learn how to conduct operations connected with the cyber domain, hence the need to practice and integrate and develop tools, in particular to recognize and create common situational awareness in cyberspace, as well as to develop platforms for cooperation and sharing information, e.g. about offensive activities. Among other issues, for this reason, in the first quarter of this year, it is planned to sign two major international agreements in the field of cyber security: an agreement with NATO on cybernetic defense (*Memorandum of Understanding*) and the development of cooperation with the US in the field of cyber security (*Cyber Defense Cooperation Roadmap*) [11].

Despite the development of allied relations, each state is obviously individually responsible for protecting its internal structures. That is why building own competences in this area is so important. Poland recently has been undertaking many initiatives related to strengthening the digital security system using the potential of Polish specialists, who according to all rankings, have been among the world leaders for several years.

This potential is successfully used in state-owned companies subordinate to the Ministry of National Defense. Enterprises such as PGZ (Polska Grupa Zbrojeniowa) or Exatel S.A. are market leaders in the field of cyber security, starting from projects related to the military use of unmanned ships (drones), through Security Operations Center services, security against DDos (distributed denial of service) attacks and Managed Firewall as well as Antimalware on related projects with the national strategic network operator.

The extent of the threat to NATO members and friendly states is vast. For example, globally the average number of devices and connections per capita will increase from 2.4 in 2017 to 3.6 in 2022 (Table 2) and the fact that among the countries that will have the highest average devices and connections per capita by 2022 are the United States (13.6), South Korea (11.8) and Canada (11.0) [1].

Table 2. Average number of devices and connections per capita

	2017	2022
Asia Pacific	2.1	3.1
Central and Eastern Europe	2.5	3.9
Latin America	2.1	2.9
Middle East and Africa	1.1	1.4
North America	8.0	13.4
Western Europe	5.4	9.4
Global	2.4	3.6

Source: [1].

Thus, the joint effort undertaken by all NATO members in the cyber domain makes the Alliance as a whole more resistant to threats in cyberspace. Poland, as a responsible member of the Alliance – is very respectful of its commitments. That is why actions are being taken in the Ministry of National Defense for making the most effective use of resources and for building optimal structures that will be responsible for building, maintaining and coordinating the Polish potential in the cyber domain.

Of course, such solutions will also require the creation of an appropriate training system enabling civilian specialists to be relatively smoothly deployed to operate in hierarchical state structures. As presented in the Kosciuszko Institute [12] report already quoted, one possible solution is the announcement of a voluntary "recruitment" of specialists to participate in both military and civil emergency response (management) exercises. Considering the level of remuneration in the Ministry of National Defense, it is likely to be assumed that financial incentives will not in most cases be the main factor taken into account by civilian specialists deciding to engage in activities to strengthen cyber security. The maximum remuneration of a civilian employee of the ministry, in accordance with the provisions of the Collective Labor Agreement for Military Employees of the Budget Sphere Organizational Units [13], is PLN 8,000 gross, although taking into account the hierarchy of civilian positions in the Ministry of National Defense, it is difficult to expect that the specialists will receive the highest remuneration rate. Remuneration for reservists appointed for military exercises are also not particularly attractive. Salaries and wages offered by the Polish Ministry of National Defense are not competitive compared to the offer of the private sector.

In order to make maximum use of human capital without "tearing" it from the work environment, one may consider cooperation with entrepreneurs specialized in cyber security, who would be willing to offer their potential to strengthen the cyber defense capabilities of the state through participation in appropriate exercises. Indeed, already there are cases where private ministries entrust private security tests, including penetration tests, to private enterprises. Furthermore, the potential of entrepreneurs associated in initiatives similar to the Polish Civic Cyber defense, has been made evident by having including them

in interdepartmental and intersectoral cybersecurity exercises, as well as in commissioning them to conduct penetration tests, simulated cyber-attacks on ICT systems, or even in developing effective methods and techniques for securing key ICT systems, based on the experience gained by entrepreneurs in resisting cyber-attacks on their own systems.

What will 2019 and next year bring?

Already at the beginning of 2019, a mega-cyber-incident occurred, this time more than 380 million records of Marriott customers unknowingly joined the world's resources of stolen information. After this incident in the United States, a discussion about the collection and processing of data was unleashed without precise rules regarding the permissible scope and period of their storage. And among other notions, regulations will be the theme in the coming 12 months. The United States is refining its RODO, and Europe will face the practical aspect of regulation introduced in mid-2018 – i.e. with penalties imposed by the regulator.

World experts in their predictions agree that more and more countries will introduce new legal regulations aimed at increasing their, and thus global security, and will also declare their readiness to join the world war in cyberspace under the pretext of defending and protecting internal critical infrastructure. Despite all efforts, efforts to build state structures to protect cyberspace, the ongoing war in this new domain will certainly lead to several hot incidents, diverting attention from current political or economic problems within countries whose cyber-troops will be involved in these conflicts.

Izabela Albrycht – President of the Kosciuszko Institute draws attention to the understanding that the security of the 5G mobile network in terms of the entire digital value chain will be one of the most important topics of the first half of the year and will be discussed and regulated by governments and international organizations such as the EU.

Another topic that will absorb the world is competition between the US and China, and the accusation that China uses the equipment it provides to customers for the purpose of illegally collecting data. The answer to this problem may be programs of certification and the independent testing of products to meet the requirements of cyber-resistance, isolating the equipment of external manufacturers (regardless of whether coming from China or another supplier), using national solutions that already exist to introduce European manufactured components as part of the security of the pan-European network, expansion of infrastructure and construction of a mobile network in 5G technology.

In such a dynamically developing field of our everyday life, it is extremely difficult to describe the threats that may occur in a few sentences. However, considering that cybersecurity is a multifaceted and intersectoral phenomenon, the best answer seems to be that we should expect what has been so far happening – but on a far larger scale.

Acknowledgement

No acknowledgement and potential founding was reported by the author.

Conflict of interests

The author declared no conflict of interests.

Author contributions

The author contributed to the interpretation of results and writing of the paper. The author read and approved the final manuscript.

Ethical statement

The research complies with all national and international ethical requirements.

ORCID

Piotr Hałys https://orcid.org/0000-0001-6557-0037

References

1. *Cisco VNI Global IP Traffic Forecast, 2017-2022*. Cisco Systems; 2018.
2. Wasilewski J. *Zarys definicyjny cyberprzestrzeni*. Przegląd Bezpieczeństwa Wewnętrznego. 2013;9.
3. Grzelak M, Liedel K. *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski*. Bezpieczeństwo Narodowe. 2012;2(22).
4. Siudak R. *Nowoczesny i innowacyjny sektor ICT. Kluczowa część krajowego ekosystemu cyberbezpieczeństwa*. In: Goździewicz W, Gutkowski C, Tabansky L, Siudak R, Skokowski D (eds.). *Bezpieczeństwo poprzez innowacje. Sektor cyberbezpieczeństwa jako siła napędowa wzrostu gospodarczego*. Kraków: Instytut Kościuszki; 2017, p. 45-56.
5. *Which Country Would Win in the Programming Olympics?*, [online]. Hacker Rank. 25 August 2016. Available at: https://blog.hackerrank.com/which-country-would-win-in-the-programming-olympics/ [Accessed: 12 May 2017].
6. *Where Should You Open Your Next Engineering Office?*, [online]. Hacker Rank. 6 April 2017. Available at: https://blog.hackerrank.com/open-next-engineering-office/ [Accessed: 12 May 2017].
7. *Polska kształci za mało informatyków. Umiejętność programowania najbardziej poszukiwaną kompetencją na rynku pracy*, [online]. Dziennik Internautów Technologie. 12 October 2015. Available at: di.com.pl/polska-ksztalci-za-malo-informatykow-umiejetnosc-programowania-najbardziejposzukiwana-kompetencja-na-rynku-pracy-53442 [Accessed: 12 May 2017].
8. *Polskie małe firmy jednak zrozumiały zagrożenie*, [online]. wGospodarce.pl. 18 June 2018. Available at: http://wgospodarce.pl/informacje/50792-polskie-male-firmy-jednak-zrozumialy-zagrozenie [Accessed: 28 March 2019].
9. Madej M, Terlikowski M (eds.). *Bezpieczeństwo teleinformatyczne państwa*. Warszawa: Polski Instytut Spraw Międzynarodowych; 2009.
10. Morańska D. *Patologie w cyberprzestrzeni. Profilaktyka zagrożeń medialnych*. Dąbrowa Górnicza: Wydawnictwo Naukowe Wyższej Szkoły Biznesu; 2015.
11. *TSA Cybersecurity Roadmap*. Transportation Security Administration; 2018, [online]. Available at: https://www.tsa.gov/sites/default/files/documents/tsa_cybersecurity_roadmap_adm_approved.pdf [Accessed: 27 May 2019].
12. Goździewicz W. *Cyberobrona i nie tylko. Rola wojska w budowaniu ekosystemu cyberbezpieczeństwa w kraju*. In: Goździewicz W, Gutkowski C, Tabansky L, Siudak R, Skokowski D (eds.). *Bezpieczeństwo poprzez innowacje. Sektor cyberbezpieczeństwa jako siła napędowa wzrostu gospodarczego*. Kraków: Instytut Kościuszki; 2017, p. 19-27.
13. *Ponadzakładowy Układ Zbiorowy Pracy dla Pracowników Wojskowych Jednostek Organizacyjnych Sfery Budżetowej. Wersja ujednolicona. Stan prawny na dzień 1 sierpnia 2011 r. uwzględniający zmiany zawarte w Protokołach Dodatkowych Nr 1-27*, [online]. Available at: http://www.wbe.wp.mil.pl/plik/file/akty/oslony/akt_199.pdf [Accessed: 27 May 2019].

Biographical note

Piotr Hałys – Col., MSc. Eng., Senior Specialist, Department of Development and Cybersecurity, Department of Science and Military Education of the Ministry of National Defense, graduate of the Tadeusz Kościuszko Military Academy of Land Forces in Wrocław, Wrocław

University of Technology, Faculty of Civil Engineering, as well as the Wrocław University of Economics, Faculty of Management, where he completed post-graduate studies. Currently, he is a PhD student at the Wrocław University of Technology at the Faculty of Mechanical Engineering. He was also a participant of several military missions in Iraq and Afghanistan, many times decorated with medals for exemplary service in the country and abroad.

Cyberprzestrzeń jako domena działalności operacyjnej i wyzwania z nią związane

STRESZCZENIE Celem artykułu jest przedstawienie współczesnych zagrożeń dla bezpieczeństwa państwa wynikających z postępującej cyfryzacji i automatyzacji kolejnych dziedzin życia, które są nie tylko o charakterze kinetycznym. Powyższy artykuł jest próbą odpowiedzi na najważniejsze pytania autora, w tym: Jak myśleć o domenie cyberprzestrzeni w całości – wojnie, pokoju i wszystkim pomiędzy? Jak rząd i sektor prywatny mogą być po tej samej stronie, jeśli chodzi o zagrożenia w cyberprzestrzeni i ich rozwiązania?

SŁOWA KLUCZOWE bezpieczeństwo, cyberprzestrzeń, bezpieczeństwo państwa, wojna informacyjna

How to cite this paper

Hałys P. *Cyberspace as a domain of operational activities and the resulting challenge*. Scientific Journal of the Military University of Land Forces. 2021;53;2(200):245-55.

DOI: http://dx.doi.org/10.5604/01.3001.0014.9780