SECURITY VERSUS THE INCLUSIVE VISION OF THE DIGITAL SOCIETY – DETERMINANTS OF SELECTED ASPECTS OF CYBER SECURITY

Joanna Grubicka[1]* Mateusz Nitka[1]
[1] Pomeranian University in Słupsk
Correspondence: joanna.grubicka@apsl.edu.pl

Abstract

An analysis of the security of the state and its citizens in terms of individual critical infrastructure systems in a situation of threats from cyberspace is one of the topics taken up by the authors of this article. As part of an experiment of a research nature conducted among students of the course Cybernetics Engineering, National Security at the Pomeranian Academy in Slupsk and students of the course Internal Security at the Kazimierz Pulaski University of Technology and Humanities in Radom, an analysis was carried out of the students' opinion of the impact of the phenomenon of cyber-terrorism on the level of national security and actions taken to combat and counteract it was presented. The article is focused on assessing the incidence of threats to critical infrastructure systems from cyberspace. The main objective of the study is to identify selected aspects of an inclusive vision of the digital society in terms of forecasting the direction of information flow and storage management in the opinion of security students of two purposefully selected universities.

Keywords: cyberspace, terrorism, cyber terrorism, national security, Poland, Internet, state security, critical infrastructure

Introduction

Ensuring the security of the state and its citizens is one of the key roles and tasks of its governing bodies. The security of an individual translates into the ability to "develop, pursue one's interests and goals while having a sense of security" (Pawłowski, Zdrodowski, 2008, p. 14).

A challenge, at the same time a threat, which has significantly intensified in recent decades, is terrorism (Macdonald, Jarvis, Lavis, 2022, pp. 727–752). This phenomenon has assumed its new form with the use of technological infrastructure

DOI: 10.5604/01.3001.0053.7155
Received: 21.03.2023 Revised: 01.06.2023 Accepted: 02.06.2023

and its tools (Ali Naqvi, Javaid, Jalal, 2022, pp. 45–57). Nowadays, all infrastructures operating in states at both civilian and governmental and military levels are based on the use of technological advances (Ghorbani, Bagheri, 2008, pp. 215–244). Due to the global nature of cyberspace, its accessibility, free availability and efficiency, all processes of daily human life have moved into the virtual world (Hoffman, 2018, p. 12). The cyberspace environment is an extremely challenging and difficult area to establish state of security due to the rapidly evolving threats and features of trans-border and anonymity.

Many states are aware of threats, the origins of which can be traced back to the existing global cyber space and evolving advances in telecommunication and communication techniques. Highly networked states are particularly vulnerable, meaning that information activity in an adversary's personal and technical information space allows them to attack their vulnerabilities in communication and information systems, categorised as critical infrastructure (Wróbel, 2019, pp. 1625–1632). They adopt and implement not only institutional and organisational but also legal solutions, which means that they attach great importance to security in cyberspace. Such documents include cyber security acts, cyber strategies, cyber security doctrines, among others. In this context, it should be noted that the catalogue of threats to state security in question has been expanded.

1. Threats in cyberspace

A negative phenomenon occurring in cyberspace is cyber-terrorism (Marsili, 2019, pp. 172–199), which entails the use of terrorist means in virtual space, with all the elements constituting terrorist activity, such as: the psychological dimension, the arousal of fear, the political nature of the phenomenon, violence or the threat of its use, etc. (Baker-Beall, Mott, 2022, pp. 1086–1105). Communication in the virtual world is increasingly frequently used by terrorist groups in order to ensure communication, the possibility of free exchange of information and coordination of activities between selected parts of the structure, during day-to-day activities, but also in moments of most important activity, such as the last phases of preparations for attacks, or during their execution. Cyber terrorism can be used in support of physical terrorist activities using cyberspace (Onat, Bastug, Guler, Kula, 2022, pp. 1–17). These activities can use virtual space to carry out cyber-attacks that cause damage, as well as destruction in the physical world, with consequences at least significant enough to give rise to fear in the community (Golase, 2022, pp. 106–119). However, cyber-terrorism solely refers to attacks in cyberspace combined with the use or threat of physical violence against persons and property (Madej, 2007, pp. 353–357).

Among the structures most vulnerable to cyber-attacks and the phenomenon of cyber-terrorism are infrastructures that are directly subordinate to the state, communities or organisations. Infrastructure assets can primarily include critical infrastructure, such as energy, fuel and water supply systems, those that produce or store various types of radioactive and chemical substances and those that ensure the continuity of public administration. Due to their nature, actions aimed at disrupting the continuity of their functioning are clearly the most frequent. A particularly vulnerable sector to cyber-attacks and disruption is the state critical infrastructure, which is underpinned by information and IT infrastructure (Danyk, Briggs, Maliarchuk, 2020). Information infrastructure comprises a collection of various networks and services. A typical information infrastructure network and services include: the Internet, public telephone networks, public data network, mobile phone networks, commercial satellite networks, radio broadcast networks, television broadcast networks, military data network, encryption devices, satellite direct broadcast television systems, online services, publishing services, financial and banking services networks, energy supply networks, transport networks, public safety networks, etc. (Gaddis, 1999, p. 5). ICT threats, together with natural and technical failures or disasters, significantly affect state security. The main activities of unauthorised persons are: remote interference with ICT systems, their paralysing or disrupting their proper operation and taking over control over them or stealing data. ICT systems belonging among others to state services, public administration, business people, but also ordinary users, may become a target of such attacks. Those systems play an important role not only in the state economy and finances, but also in the proper functioning of critical infrastructure (Grubicka, 2020, p. 136). In terms of state security, it is up to the system to determine the degree of threat of a given cyber attack. The severity of electronic attacks also varies. Hacking into a single website or administrative site has different consequences than those while hacking nationwide networks, payment systems or the network of a central office. The motivation, character and skills of the perpetrator also play an important role; they are the main determinants of how network attacks impact state security (Grubicka, 2020, p. 137). Actions by individuals who just want to test their skills will pose a different threat, while those of a political nature, such as the actions of terrorist groups, will most likely be different (Madej, Terlikowski, 2009, pp. 95–96). As a result, new types of threats have emerged, such as cybercrime, cyber terrorism, cyber espionage or cyber warfare, in the sense of clashes between states in cyberspace and other types of cyber conflict. Current trends in the emergence of cyber threats point to a large extent to the impact of the level of security in cyberspace in relation to the overall security of the state. The increasing dependence on technology means that conflicts in the virtual world can become a serious source of malfunctioning of societies and states (Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, 2014, p. 19).

The range of ICT activities has positive as well as negative effects. Currently, the positive effects include social communication, creation of tools for learning, entertainment, among others. Negative effects of activities include: cyber surveillance, cybercrime, cyber warfare, cyber terrorism (Sienkiewicz, 2009, p. 98).

According to the CISCO report, attacks conducted in a serial mode are increasingly burdensome in terms of frequency and duration. Among surveys conducted in this regard, more than 42% of respondents were convinced that their organisations had been victims of DDoS attacks in 2017 (www.cisco.com, 2022). The report highlights the fact that malware is evolving and becoming much more disruptive and harder to combat.

All analyses carried out by CISCO in 2021 were aimed at preparing a spreadsheet of potential threats for 2022. At the beginning of the document, it was mentioned that experts in charge of cyber security have had to deal with most of the possible incidents that can occur in cyberspace this year (www.techno-senior.com, 2022). Even experts, including analysts, often become victims of harassing messages or receive links that, if clicked on, could result in infecting not just a single computer, but the entire internal network (www.blog.talosintelligence.com, 2022). One of the main elements helping cybercriminals was the constant filtering of the latest news and research concerning gaps in IT systems and security of enterprises, banks and social networks. In this way, they compile information about potential future systemic failures and deploy them in their attacks (Khodjibaev, Korzhevin, McKay, 2021, p. 3). In the opinion of criminals, hospitals and schools are particularly vulnerable units to ransomware attacks due to their low resilience against threats from the Internet. These units are very poorly funded in terms of having their own specialists, yet they are a very good potential source for attack in terms of stored data, such as residing patients. It is considered that it is the individual units that are the weakest links in maintaining cyber security. It is the human factor and its errors that mainly contribute to the vulnerability of cyber security systems to attacks.

A further threat is the state energy sector. It consists of enterprises and companies involved in the acquisition, generation and transmission of electricity. In Poland, there is the National Power System, the subsystems of which include the generation subsystem and the transmission and distribution networks (Polska Agencja Informacji i Inwestycji Zagranicznych, 2022, p. 1). Due to the daily energy demand and the high level of dependency between all other subsystems and the power sector, it is one of the most important targets for cyber-terrorist attacks. The transmission grid distributes energy throughout the country. When a potential cyber-attack on the transmission network structure below occurs, the rest of the entities that make up the national security system will become immediately affected.

The basis of ICT system security is a well-prepared security system design. Using already developed standards and regulations makes it much easier to create from scratch or modify the existing security architecture. STIG, an acronym for Security Technical Implementation Guide, is a very comprehensive and up-to-date standard (Muniz, Lakhani, 2013, p. 254). It comprises a set of standards that define the methodology of the installation, operation and management of computer hardware and software. The guidelines were developed for the US Department of Defence by the government Defence Information Systems Agency

(DISA) and continue to be developed and updated by DISA (www.public.cyber.mil, 2022). The STIG recommendations outline how to significantly improve chances of a system of repelling attacks and how to minimise the losses in the event of a successful penetration of the security system. The standards also define processes involved in administering operating systems, such as software updates and installing security patches. The guidelines also provide a starting point for non-standard configurations - those that must meet strict requirements imposed by legal or industry standards. In the US, all devices operating under the control of the Department of Defence (Littlejohn Shinder, Tittel, 2004, p. 51) are required to comply with STIG standards. An essential factor in establishing the suitability of a deployed security system in operation is to perform oversight and manage it while continuing its development. The efficiency of a security system is achieved by the ongoing elimination of vulnerabilities, upgrading the skills of users and testing the implemented protection. A system is considered to be consistent if one or more safeguards exist for each vulnerability. Therefore, a properly constructed protection system, supported by legal and organisational solutions, adhering to the principles defined by the information security policy, allows the state to fulfil its internal and external functions. “National security of states is increasingly dependent on the efficiency of the information infrastructure (including ICT infrastructure). Its collapse can cause a calamity, the magnitude of which keeps increasing every year. The threat of such a development is posed by both the complex nature of functional links and internal couplings of the state information infrastructure and the exponential development of ICT. In the opinion of many specialists, the collapse of the functioning of state information infrastructure (including ICT infrastructure) would lead to the disorganisation of state functioning and a threat to its interests in the world” (Gaddis, 1999, p. 5).

Regardless of the IT aspects of cyberspace and the security of each entity (including the state), information is of strategic importance. Its usefulness allows authorized entities to perform complex tasks in personal and technical information space essential for the efficient functioning of the state. This allows threats to be prevented or minimised in a globalised military and non-military security environment.

The National Security Strategy is the concept in force in the state for ensuring its security, which includes, in particular, the identification of national interests and strategic objectives, an assessment of the future formation of the strategic security environment and the principles and ways of achieving strategic objectives in the envisaged conditions (implementation of operational tasks), as well as the preparation (maintenance and transformation) of the national security system (implementation of preparatory tasks). The National Security Strategy is the basic document establishing the conceptual foundations of the organisation, preparation and functioning of the national security system in times of peace, threat and war in accordance with their own national interests and according to the existing conditions.

The current National Security Strategy of the Republic of Poland is a document approved in Warsaw on 12 May 2020 by the President of the of the Republic of Poland at the request of the Prime Minister. The document was issued on the basis of article 4a section 1 item 1 of the Act of 21 November 1967 on the general duty to defend the Republic of Poland. It contains a definition of the basic interests and objectives of the Polish state in the field of national security. The security concept presents an approach to the issue of threats and covers not only purely military threats. This strategy is in line with the objectives of NATO and the European Union, as well as with the Constitution of the Republic of Poland. The various dimensions relating to national security are external, military, internal, civic, social, economic, environmental, information and telecommunications security. The document emphasises the strengthening sense of national identity with equal integration of the Poles.

A very significant and quite likely the most important shortcoming of the current security strategy is the lack of an operational strategy, i.e. strategic objectives and tasks regarding the ways of counteracting threats (including war threats) and risks, taking up challenges or making use of opportunities for Poland's security established by the strategic environment. The strategy present in the task part is only a preparatory one. It applies to the ways of preparing (development, improvement) particular segments of the national security system. However, it does not define the purpose of these preparations and what they are to serve. It does not indicate either how Poland is to prevent threats, what its priorities will be in relation to crisis threats, whether it has to take into account an independent defence response in certain scenarios, how it can counter subliminal aggression, whether and how it intends to conduct widespread resistance on territories occupied by the aggressor, etc.

The National Security Strategy of the Republic of Poland defines four strategic pillars:

1) Security of the state and citizens;
2) Poland's actions in the international security system;
3) National identity and heritage;
4) Social and economic development.

Among other things, the first pillar lists two objectives of the strategy, i.e. cyber security and information space. The text of the document indicates that various measures would be taken in these areas to anticipate and mitigate threats. This includes the goal of increasing cyber resilience to cyber threats and enhancing the level of information protection in the public, military, private sectors and promoting knowledge and good practices to enable citizens to better protect their information. In addition, the strategy points to the need of increasing the resilience level of information systems used in the public and private, military and civilian spheres and to achieve the capacity to effectively prevent, combat and respond to cyber threats. Corresponding to this is the assumption that the defensive potential of the state should be strengthened by ensuring the continuous development of the national cyber security system and by achieving the ability of conducting a full spectrum of military operations in cyberspace. The strategy goes on to point out the need of developing national capabilities in the field of testing, research, evaluation and certification solutions and services in the area of cyber security, and also the development of competence, expertise and awareness of threats and challenges among public administration personnel, as well as in society in the area of cyber security (Grubicka, 2019, pp. 96–97). It seems very important to refer to the inevitable requirement of strengthening and expanding Poland's potential by, inter alia, developing domestic solutions in the field of cyber security and conducting state-funded research and development in the area of modern technologies, including machine learning, the Internet of Things, fixed and mobile broadband communication networks (5G and subsequent generations), along with cooperation with universities and scientific institutions and enterprises - both from the public and private sector.

In terms of the objective referred to as 'information space', the strategy focuses on ensuring the secure functioning of the state and of the citizens in the information space and building, at the strategic level, the capacity to protect the information space (including the systemic fight against disinformation), understood as the interpenetrating layers of space: virtual (the layer of systems, software and applications), physical (infrastructure and hardware) and cognitive (cognitive). It is becoming necessary to establish a unified strategic communication system of the state, the task of which should be to forecast, plan and implement coherent communication activities, using a wide range of communication channels and media along with the utilisation of reconnaissance tools, as well as influencing various areas of national security. The strategy also assumes that disinformation should be actively countered by building capacity and creating procedures for cooperation with news channels and social media, with the involvement of citizens and NGOs. It also appears that striving to increase public awareness of the risks associated with information manipulation through education in the field of information security is also an important objective.

A suitable plan is needed in order to effectively combat cybercrime. The first step is to appropriately define the problem. A further step is to compile statistical data necessary for the analysis. The final step in the fight against cybercrime is to educate both the crime-fighting teams as well as people who are victims of cybercrime, e.g. IT professionals, forensic professionals and the entire society (Littlejohn Shinder, Tittel, 2004, p. 51). According to J. Kosinski, the proposed model of a cybercrime fighting system consists of three phases: network investigation, on-scene activities and digital evidence analysis. More complex tasks aimed at combatting cybercrime require the joint work of several teams:

- operational-investigative team;
- reaction-investigation team;
- forensic laboratory team;
- research and development team.

> In order to streamline the whole process, the cooperation of the above-mentioned teams is essential, also if in a case that is pending the digital device is only a carrier of data that may be relevant to the case (Kosiński, 2015, pp. 213–216). The formations responsible in Poland for combating computer crime of a criminal nature are the police and the military police. Events of a terrorist and espionage nature on the Internet are dealt with by the Internal Security Agency (ABW) and Military Counterintelligence Service (SKW). "On the other hand, the entire coordination of activities is handled by the Interdepartmental Coordinating Team for the Protection of the Cyberspace of the Republic of Poland, whose representatives include five ministries (Ministry of Science and Higher Education, Ministry of National Defence, Home Office, Ministry of Infrastructure), the Police Border Guard, the State Fire Service, the Internal Security Agency, the Government Security Centre and the Military Counterintelligence Service" (Kosiński, 2015, pp. 233–234). The cyberspace security plenipotentiary is responsible for managing the work of the team, while plenipotentiaries are to be appointed in public administration units to perform tasks included in the cyber security of the Republic of Poland.

In order to fight cybercrime more effectively, Internet solutions have recently been implemented, which are to contribute to a decrease in the number of crimes committed online. An example of such a tool is the INDECT project, coordinated by the Department of Telecommunications at the AGH University of Science and Technology in Kraków. It aims to detect real threats, e.g. via cameras, as well as virtual ones (in computer networks and the Internet). A further tool is the INACT project, which is a whole set of programmes designed to combat the illegal production and distribution of child pornography content. Another of the tools is INCR (INDECT Crawler). It scans automatically Internet resources, focusing on given symbols (e.g. the swastika). These tools have been developed to assist in the fight against cybercrime and relieve the burden on other units dealing with this subject (Hołyst, 2012, pp. 99–110).

The entire cyber activity has a huge impact on the level of national security (Backhaus, Gross, Waismel-Manor, Cohen, Canetti, 2020, pp. 595-603). National security is made up of executive subsystems that are closely interconnected. If an attack on one operating system is successful, it has an immediate impact on the level of national security (Shandler, Gross, Backhaus, Canetti, 2022, pp. 850–868).

Despite the ICT system developed in accordance with recognized security methods, no absolute security is feasible. There are no methods to guarantee total information security. If attacks by cyber criminals become inviable as a result of an adequate degree of security, i.e. the cost of acquiring protected information exceeds its value, data may still be at risk as a result of a cataclysm, military action or other unforeseen events, including random events.

2. Significance of the impact of cyber crimes and cyber-terrorist threats on the level of national security in Poland in the opinion of students of national security

2.1 Research assumptions

The essence of the research problem was the perception of the impact of cyber crimes and cyber-terrorist threats on the level of national security in Poland in the opinion of students majoring in the field of national security at two selected universities given geopolitical location. The research was conducted in the period of April-June 2022 and comprised a group of students from the Pomeranian Academy in Słupsk (232 students) and the Kazimierz Pułaski University of Technology and Humanities in Radom (89 students) studying Cyber Engineering, National Security and Internal Security. The students took part in an experiment as part of their research and implementation of a research project: Cyber security in the aspect of contemporary threats. As part of the series of monographic lectures on: *Prolegomena of cyberspace – consequences of technological and human development in a media civilisation*. The main objective of the research is to seek an answer the question of the state of students' knowledge of the state security of critical infrastructure systems in the face of threats using cyberspace, and also to attempt to develop the results of the research on forecasting the direction of the flow of management and storage of information on the level of state cyber security. The selection of the sample was examined for a random group of two universities in different geopolitical spaces. The authors of the posters draw attention to the characteristic features of a given area: in Radom, due to the airport, and in Słupsk, evidence of the anti-missile shield in Redzikowo. The study was carried out using the CAWI method (Computer-Assisted Web Interview) and a survey questionnaire in the research group.

2.2 Analysis of research results

From the analysis of the developed material it is apparent that approx. 59.6% of the students remained convinced that technological development has a considerable impact on the development of cyber threats. Approximately 34% were of the opinion that it has a substantial impact and only about 6.4% say that it has a negligible impact on the development of cyber threats. The majority of the respondents in the number of approx. 40.4% said that they were not likely to become the target of a cyberattack, about 19.1% are those who suppose that they might have been, although they were not sure about it, and 17% say that they were a target of such a cyberattack, about 14.9% are sure that they were not the target of cyberattacks, while 8.5% are those who are sure that they were a target. Some 48.9% of the respondents feel a real threat related to the security of their data when using the Internet, 27.7% definitely feel such a threat, and 19.1% of respondents do not feel a threat, while 4.3% definitely do not.

Approximately 51.1% of students believe that the websites that store their data have adequate security systems, 12.8% are convinced that they definitely do not have such security systems, 34% are of the opinion that the websites that hold their data have such security systems, 2.1% say that they definitely do. The severity of a citizen's exposure to the threat of cyber espionage when transmitting their data online was determined on a scale of 1–5 (low–high) by: 5–27.7%, 4–34%, 3– 31.9%, 2–4.3%, 1–2.1%. The majority of respondents, i.e. approx. 53.2%, believe that the consequences of criminal activity, including extortion, fraud and theft, could seriously threaten the functioning of Poland in the future.

On a scale of 1 to 5 (1 being negligible and 5 indicating very high), the respondents indicated to what extent the ICT space allows terrorists to plan attacks and execute terrorist ventures. The respondents were given multiple-choice options to tick. The most vulnerable sector to cyberattacks in terms of information held and compiled, according to the students, is the public sector - 63.8%, followed by the private sector at 46.8%, with the least vulnerable being citizens as an individual, around 34%. One of the most vulnerable sectors to cybercriminal activity in the future according to the respondents will be the financial sector (53.6%), followed by the energy sector (24.2%), transport (36.2%), insurance (27.7%), retail (25.5%) and the least vulnerable sector is wholesale (21.3%).

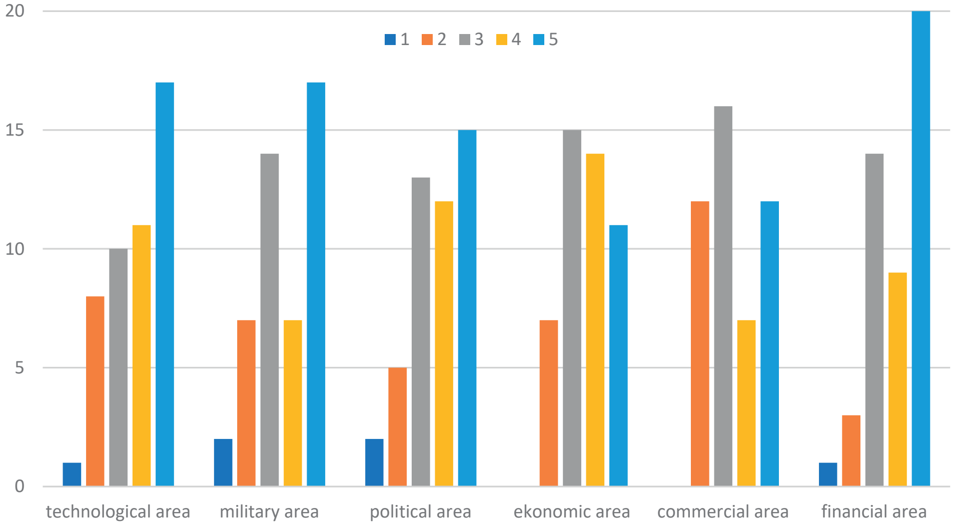

Figure 1. Degree of exposure of individual areas to cyber espionage threats on a scale of 1 to 5, 1 indicating negligible, and 5 indicating very high

Fig. 1 shows the areas vulnerable to cyber espionage. The students responded on a scale of 1 to 5, where 1 indicates a negligible level and 5 a very high one. According to the respondents the most susceptible area is the financial sector, a very high threat level of 5 to 19.8%, and the least is the commercial area.

The vulnerability level to cyber threats of critical infrastructure systems (scale of 1 to 5, 1 – negligible level, 5 – very high), the respondents assigned the highest score (very high) to communication systems together with systems that guarantee the continuity of public administration and production systems including storage of radioactive, chemical and hazardous substances, the financial area (about 19.89%), 9% of votes both for rescue systems and food and water supply systems.

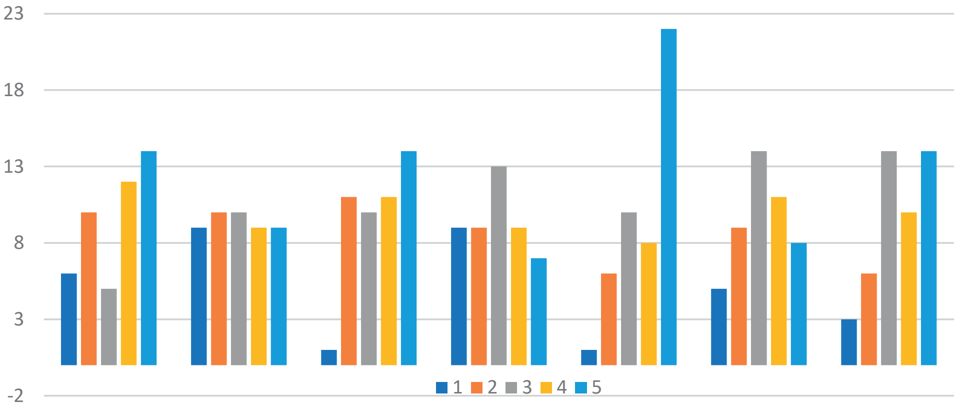

Fig. 2. The degree of exposure of individual critical infrastructure systems to threats from cyberspace on a scale from 1 (negligible) to 5 (very high). From left, in order: production systems including storage of radioactive, chemical and hazardous substances, systems providing food and water supply, systems guaranteeing the continuity of public administration, rescue systems, financial systems, raw material supply systems, communication systems

Another aspect of the research concerned future risks. Students were able to make multiple choices on the given problem context. The areas that will require the most attention in the opinion of the students comprise security of critical infrastructure (72.3%) and modernisation of law enforcement technical facilities 69.6%. This is followed in descending order by the areas of legal regulation (48.9%), ethical aspects of artificial intelligence (36.2%), promotion of ethical attitudes (25.5%) and a low level of the wealth of society (17%).

According to the respondents, the majority of cyberattacks are caused by criminal groups, ca. 42.6%, followed by terrorist groups - 31.9%, ordinary people (17%), and the least special state units (8.5%). The creation of a specialised further education programme in the field of information security would definitely have impact on a broader perception of cyber security threats by citizens (47.8%), while 43.5% would rather have an impact. Some 6.5% think it would most likely not have an impact and 2.2% think it would definitely not have an impact.

A rating scale of 1 to 5 was also adopted to examine factors that may influence the increase of the level of security in cyberspace. According to the respondents to the research experiment, some 21% of them believe that these include investing by the State in new technologies and cyber security specialists, and establishing uniform international rules in the sphere of prosecuting cyber criminals (25%), developing awareness of threats among citizens (17%), developing alert systems for monitoring online movements (8.3%), social campaigns (0.7%) and restricting freedom of movement on the Internet (29%).

46.8% of respondents say that a cyber threat exists in Poland, 42.6% of the students are strongly inclined, and 10.6% think that there is no such threat.

Polish authorities seem to be inadequately prepared to prevent and counter cyberattacks according to the majority of respondents (51.1%), (21.3%) of them say definitely yes (25.5%), (2.1%) say definitely no.

The correlation between the students of the Pomeranian Academy of Słupsk and the Kazimierz Pułaski University of Technology and Humanities of Radom regarding the impact of cyber threats and cyber terrorism on the level of national security in Poland was also examined.

Considering the case of measuring the correlation between the knowledge/perceptions of students from a given university (xi) and the degree of proficiency in managing the flow and storage of information conditioning the level of state cyber security (y_i), the value of the r-Spermann correlation coefficient for these pairs of variables is $r_{xyAP} = 0.83$ for $r_{xyRANDOM} = 0.79$. The variables were assigned ranks, ordered by degree of skill (y_i) in ascending order. Interpreting the correlations, it can be concluded that a very high correlation exists. The student's knowledge of both AP Słupsk and UTH Radom appear to converge.

Summary

The need for the safe and proper functioning of cyberspace requires the state to make the area of cyberspace functioning a priority in national security policy, and for the state itself to attempt to effectively create systems to counter threats at the strategic, legal and institutional levels.

Cyber-terrorism is a negative effect of ICT activities caused intentionally by a human being, often with the aim of extorting ransom, creating a feeling of fear and panic among citizens, as well as upsetting the level of national security through attacks on critical infrastructures or achieving given ideological goals. What is more, due to its characteristic features, i.e. anonymity and easy accessibility to the Internet, it represents one of the most evolving threats of the 21st century, and a challenge for law enforcement agencies, as it also has a cross-border nature, which makes the process of prosecuting the criminals responsible for these phenomena even more difficult.

Several important conclusions can be drawn from the material presented in this article:

1. The national security structures of Poland are exposed to the phenomenon of cyber-terrorism.
2. The consequences of criminal activities, including extortion, fraud and theft, may seriously threaten the functioning in Poland in the future.

3. There is definitely a cyber-terrorist threat in Poland, regardless of geopolitical location. Polish authorities are inadequately prepared to prevent and counteract cyberattacks. Given the key role of information in today's society, the problems identified should be addressed with the highest priority. The development of the information society must go hand in hand with the development of methods of ensuring security and raising user awareness.
4. However, measures taken to protect cyberspace will never be sufficient for any entity to feel fully secure. The infinite number of existing risks, with insufficient solutions contributing to their security, does not inspire optimism.
5. One of the most important challenges in the field of cyber security is to counteract threats at strategic, legal and institutional levels on possible threats in cyberspace related to the changing world and the increasing and more widespread access to modern technologies.

Threats specific to Słupsk and its vicinity differ from those in Radom due to their geopolitical location. In Radom, special attention may be paid to the threats to the airport facility and the surroundings, and in Słupsk and the immediate area, the anti-missile shield base. In the opinion of students of the field of Cyber Engineering, National Security and Internal Security, cyberspace provides conditions for terrorists to carry out their ventures and plan terrorist attacks to a very high or high degree. The public sector is the most vulnerable to threats posed by cyberspace in terms of information held and collected. Vulnerable sectors exposed to cybercrime activity are the in the first place the financial sector, the energy sector and transport. Particularly vulnerable sectors exposed to cyber espionage activities are the financial, technological, military and political areas. The areas exposed to threats from cyberspace include the financial, political, military and economic areas. Vulnerable critical infrastructure systems include financial systems, communication systems, systems guaranteeing the continuity of public administration and production systems including the storage of radioactive, chemical and hazardous substances. Areas including the security of critical infrastructure, modernization of technical facilities of law enforcement agencies and legal regulations require particular attention in the context of prospective threats. According to the vast majority of respondents, threats that arise from cyberspace will definitely keep evolving. The development of a specialized training program in the field of information security would definitely contribute to the wider awareness of cyber security threats by citizens. State investments in new technologies and cyber security specialists, establishing uniform international regulations in the field of prosecution of cybercriminals and developing awareness of threats among citizens may contribute to the increase of the level of cyberspace security.

Post-conference paper: "Crisis and organization of homeland security in the face of contemporary threats. New challenges of the digital society".

References

1. Ali Naqvi A., Javaid, A., Jalal, I., (2022). From Cyber Security to Cyber-terrorism: A New Emerging threat for Europe and the challenges for EU. *Journal of Politics and International Studies*, Vol. 8, no 2.
2. Backhaus, S., Gross, M. L., Waismel-Manor, I., Cohen, H., & Canetti, D., (2020). A cyberterrorism effect? Emotional reactions to lethal attacks on critical infrastructure. *Cyberpsychology, Behavior, and Social Networking*, 23(9).
3. Baker-Beall, C., & Mott, G., (2022). Understanding the European Union's Perception of the Threat of Cyberterrorism: A Discursive Analysis. *JCMS: Journal of Common Market Studies*, 60 (4).
4. Danyk, Y., Briggs, C., & Maliarchuk, T., (2020). Features of Ensuring Cybersecurity of the Critical Infrastructure of the State. *Theoretical and Applied Cybersecurity,* 2(1).
5. https://blog.talosintelligence.com/2021/01/nation-state-campaign-targets-talos.html [30.11.2022].
6. https://techno-senior.com/2022/01/12/cisco-2021-podsumowanie-cyberzagrozen [30.11.2022].
7. https://www.cisco.com/c/m/pl_pl/products/security/security-report.html [30.11.2022].
8. Gaddis, J.L., (1999). Bezpieczeństwo Stanów Zjednoczonych w świetle walki informacyjnej. *Wojskowy Przegląd Zagraniczny*, No 3.
9. Ghorbani, A.A., & Bagheri, E., (2008). The state of the art in critical infrastructure protection: a framework for convergence. *International Journal of Critical Infrastructures*, 4 (3).
10. Golase, P.R., (2022). A Comparative Analysis of the Factors Predicting Fears of Terrorism and Cyberterrorism in a Developing Nation Context, *Journal of Ethnic and Cultural Studies*, 9 (4).
11. Grubicka, J., (2019). Information society in the context of threats to personal security in cyberspace. *Zeszyty Naukowe Politechniki Śląskiej Organizacja i Zarządzanie*. Issue 141.
12. Grubicka, J., (2020). Świat w sieci – nowa jakość zagrożeń dla bezpieczeństwa państwa. In: Molendowska, M., Miernik, R., (eds.), *Bezpieczeństwo w cyberprzestrzeni*, Warsaw: Adam Marszałek Publishing House.
13. Hoffman, T., (2018). Główni aktorzy cyberprzestrzeni i ich działalność, In: *Cyberbezpieczeństwo wyzwaniem XXI wieku*, Dębowski, T.R. (ed.), Łódź–Wrocław: ArchaeGraph.
14. Hołyst, B., Pomykała, J., (2012). *Cyberprzestępczość i ochrona informacji.* Vol. I. Warsaw: Wydawnictwo Wyższej Szkoły Menedżerskiej.
15. Khodjibaev, A., Korzhevin, D., McKay, K., (2021). *Interview with a LockBit ransomware operator*, *Talos Cisco Security Research*.
16. Kosiński, J., (2015). *Paradygmaty cyberprzestępczości*. Warsaw: Difin.
17. Littlejohn Shinder, D., Tittel, E., (2004). *Cyberprzestępczość. Jak walczyć z łamaniem prawa w sieci*. Gliwice: Helion.
18. Macdonald, S., Jarvis, L., & Lavis, S. M. (2022). Cyberterrorism today? Findings from a follow-on survey of researchers, *Studies in Conflict & Terrorism*, 45 (8).

19. Madej M., (2007). *Zagrożenia asymetryczne państw obszaru transatlantyckiego,* Warsaw: Polski Instytut Spraw Międzynarodowych.
20. Madej M., Terlikowski M. (2009). *Bezpieczeństwo teleinformatyczne państwa*, Warsaw: Polski Instytut Spraw Międzynarodowych.
21. Marsili, M., (2019). The war on cyberterrorism. *Democracy and security*, 15 (2).
22. Muniz, J., Lakhani, A., (2013). *Web Penetration Testing with Kali Linux*, Birmingham: Packt Publishing.
23. Onat, I., Bastug, M.F., Guler, A., & Kula, S., (2022). Fears of cyberterrorism, terrorism, and terrorist attacks: an empirical comparison. *Behavioral Sciences of Terrorism and Political Aggression*.
24. Pawłowski, J., Zdrodowski, B. (2008). *Słownik terminów z zakresu bezpieczeństwa narodowego*. Warsaw: Wydawnictwo Adam Marszałek.
25. Polska Agencja Informacji i Inwestycji Zagranicznych S.A., *Sektor energetyczny w Polsce*.
26. Shandler, R., Gross, M.L., Backhaus, S., & Canetti, D., (2022). Cyber terrorism and public support for retaliation – a multi-country survey experiment, *British Journal of Political Science*, 52(2).
27. Sienkiewicz, P., (2009). *Terroryzm w cybernetycznej przestrzeni*. In: Jemioła, T., Kisielnicki, J., Rajchel, K., (ed.) *Cyberterroryzm. Nowe wyzwania XXI wieku*, Warsaw.
28. Standardy STIG – aspektów bezpieczeństwa teleinformatycznego. https://public.cyber.mil/stigs/downloads [02.12.2022]
29. *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* (2014), Warsaw: BBN.
30. Wróbel, R., (2019). Dependencies of elements recognized as critical infrastructure of the state. *Transportation Research Procedia*, No 40.

BEZPIECZEŃSTWO A INTEGRACYJNA WIZJA SPOŁECZEŃSTWA CYFROWEGO – UWARUNKOWANIA WYBRANYCH ASPEKTÓW CYBERBEZPIECZEŃSTWA

Abstrakt

Analiza bezpieczeństwa państwa i jego obszarów w zakresie poszczególnych systemów infrastruktury krytycznej na zagrożenia pochodzące z cyberprzestrzeni jest elementem dyskursu autorów artykułu. W ramach prowadzonego eksperymentu o charakterze badawczym wśród studentów kierunku Inżynieria Cyberprzestrzeni, Bezpieczeństwo Narodowe Akademii Pomorskiej w Słupsku oraz studentów kierunku Bezpieczeństwo Wewnętrzne Uniwersytetu Technologiczno-Humanistycznego im. Kazimierza Pułaskiego w Radomiu przedstawiono analizę wpływu zjawiska, jakim jest cyberterroryzm, na poziom bezpieczeństwa narodowego oraz działania podejmowane ku jego zwalczaniu i przeciwdziałaniu w ocenie studentów. Artykuł poświęcony jest ocenie wystąpienia zagrożeń w zakresie systemów infrastruktury krytycznej pochodzących z cyberprzestrzeni. Głównym celem opracowania jest wskazanie wybranych aspektów integracyjnej wizji społeczeństwa cyfrowego o prognozowaniu kierunku zarządzania przepływem i magazynowaniem informacji w opinii studentów kierunku bezpieczeństwa dwóch celowo wybranych uczelni.

Słowa kluczowe: cyberprzestrzeń, terroryzm, cyberterroryzm, bezpieczeństwo narodowe, Polska, Internet, bezpieczeństwo państwa, infrastruktura krytyczna