European Integration Studies, Volume 20, Number 2 (2024), pp. 137-159.
https://doi.org/10.46941/2024.2.6

BARBARA KACZMARCZYK[*]

Cybersecurity from a systemic perspective**

ABSTRACT: Cyberspace has become a place of aggressive attacks aimed at various areas of human life. Statistics indicate a dynamic increase in cyberattacks in European Union (EU) member states and NATO countries, where technologies are developing at a rapid pace; on the one hand, this contributes to economic growth and, on the other hand, to the creation of increasingly complex cyberattack algorithms. They are aggressive and can cause significant losses.

The following research methods were used to develop the article: analysis and synthesis of literature on the subject in the field of security, the state security system, cybersecurity, statistical data and legal acts. interviews were also conducted with experts in the field of security and cybersecurity systems.

A systemic approach can be considered in the context of two subsystems: management and executive. The management subsystem includes the decision-making bodies of NATO and EU structures that develop a cybersecurity policy for all members of their structures, while the executive subsystem includes the armed forces and other security entities of individual EU and NATO members, as well as society on an individual (citizens) and collective (private institutions, enterprises) basis.

Due to the nature of cyber threats, cyber security should be considered systemically, i.e. in a way that covers all its aspects; we should also improve cybersecurity strategies to counter threats, secure infrastructure and the green energy sector, develop technological and production resources, and enable the creation of cyber defense that is applicable both in one country and around the world.

[*] PhD., Associate professor in the field of social sciences in the discipline of security science in the field of social sciences in the discipline of security science, General Tadeusz Kościuszko Military University of Land Forces, Poland, ORCID: 0000-0002-6995-2961, barbara.kaczmarczykwso@gmail.com.

[**] The research and preparation of this study was supported by the Central European Academy.

KEYWORDS: cyberspace, threats in cyberspace, cybersecurity, information, military sector, civilian sector, system.

1. Introduction

Threats in cyberspace are unpredictable and have no borders, which means that their scope is global, and they can cause significant losses in all important areas of human life. These factors affect the security of both countries and the world. Cyber incidents have become particularly important in the face of a dynamically developing world in which new-generation technologies create new opportunities for action. Therefore, the approach to this issue must have a holistic dimension: exploration of phenomena and event processes. The first and most important assumption is that everyone is responsible for security, including cybersecurity. This encompasses public institutions and bodies, non-governmental organisations, private sector institutions, and citizens. The effectiveness of actions is determined by many factors, one of them being the strategies that set the course of action to face threats and help secure the future of cyberspace. To ensure security on the Internet, countries develop cybersecurity strategies and legal provisions and cooperate with other countries.

The aim of these activities is not only the security of ordinary citizens, groups, nations, or nations but also the possibility of functioning in countries that have the ability to counter threats, develop the green energy sector, and develop economic and technological sectors. Internal and external cooperation remains an important element, as does everyone’s awareness of the defence against cyberthreats. An action strategy should adopt systemic solutions that are similar across all countries. The National Cybersecurity Strategy, published by the Biden–Harris administration, announced on 2 March 2023, includes many aspects that can be included as elements of this system.[1] It focuses on building cooperation based on the defence and protection of critical infrastructure, effective use of technology, involvement of private entities, investments in resilience, and international

[1] USA – National Cybersecurity Strategy, 2024, [Online]. Available at: https://cyberpolicy.nask.pl/usa-krajowa-strategia-cyberbezpieczenstwa/ (Accessed: 30 January 2024).

cooperation.[2] This approach is multifaceted and needs to be accurately defined.

In the opinion of the author and surveyed experts in the field of cybersecurity, this issue should be considered systematically. The systemic approach to security considerations, including cybersecurity, is supported by its features such as (a) holism (perceiving phenomena and processes as a whole), (b) comprehensiveness (revealing various connections and internal relations), (c) essentialism (studying phenomena or objects from the viewpoint of important characteristic features), (d) structuralism (identifying the properties of an object or area of interest based on those features of its structure that are considered unchanging and integrating), (e) contextuality (considering systems according to their place in a larger whole), (f) teleologism (considering phenomena from the viewpoint of their purposefulness in a given field, especially in reality), (g) functionality (considering systems in terms of the goals achieved and fulfilling functions), (h) effectiveness (considering systems from the perspective of the size of the results achieved and goals and functions performed), (i) synergism (consideration of properties resulting from cooperation and cooperation within the system of subsystems and elements of these subsystems, the essence of which is cooperation, which is more effective than the sum of their separate activities), and (j) development (consideration of systems in approach to transformations and changes related to the transition to states or forms that are more complex or, in some respects, more perfect).[3] These system features are important when considered individually and collectively. They are so important that the issue of cybersecurity should be discussed considering all features related to the concept of the 'system'.

This study aims to comprehensively consider cybersecurity by considering the characteristics of the system. Therefore, in the context of the above, the research problem was defined as 'What assumptions should be made when defining the cybersecurity system and which of its elements (subsystems) play a key role in ensuring security'.

For this study, it was assumed that a cybersecurity system is a set of forces and resources understood as personal and material resources allocated by the state or states to carry out security tasks in cyberspace. This system

[2] Ibid.

[3] Wiśniewski, 2013, pp. 115–116.

consists of a management subsystem and an executive subsystem,[4] which includes the operational and support sectors. The operational sector includes the defence and protection departments, whereas the support sector includes the social and economic departments. Based on the above assumptions, a discussion of cybersecurity is undertaken from a systemic perspective.

2. Assumptions of the cybernetic security system – the management subsystem

European security systems are based on several interconnected components, as follows: (a) the North Atlantic Alliance (NATO),[5] (b) the European Union (EU) with its Common Security and Defense Policy (CSDP),[6] and (c) the Organization for Security and Co-operation in Europe (OSCE).[7] NATO is treated as a political and military organisation capable of using its force to defend member states and strengthen the geopolitical bond between the United States and Europe by guaranteeing their presence on the European continent, which is strategic for European security in both political and military contexts. The role of the EU is to integrate its members and cooperate intensively and effectively with NATO. In turn, OSCE activities have focused mainly on the territory of the former USSR and have been limited because of Russia's policy. Therefore, it was considered that OSCE's participation in European security activities was marginalised.[8]

The management subsystem is a key element in the discussion of the cybersecurity system and is designed to direct its functioning. This includes the EU and NATO, which outline international cybersecurity policies within their structures. This subsystem is responsible for the implementation of groups of tasks such as (a) monitoring incidents and attacks in the network (the scale of their occurrence, trends, their nature, type, and place of

[4] White Book of National Security of the Republic of Poland, 2024, [Online]. Available at: chat.openai.com, p.36; (Accessed: 30 March 2024).

[5] NATO Communications and Information Agency, [Online]. Available at: https://www.nato.int/cps/en/natohq/topics_78170.htm (Accessed: 23 April 2024).

[6] The Common Security and Defence Policy, [Online]. Available at: https://www.eeas.europa.eu/eeas/common-security-and-defence-policy_en (Accessed: 23 April 2024).

[7] Organization for Security and Co-operation in Europe, [Online]. Available at: https://www.osce.org (Accessed: 23 April 2024).

[8] White Book of National Security of the Republic of Poland, 2024, [Online]. Available at: chat.openai.com, pp.123-127. (Accessed: 30 March 2024).

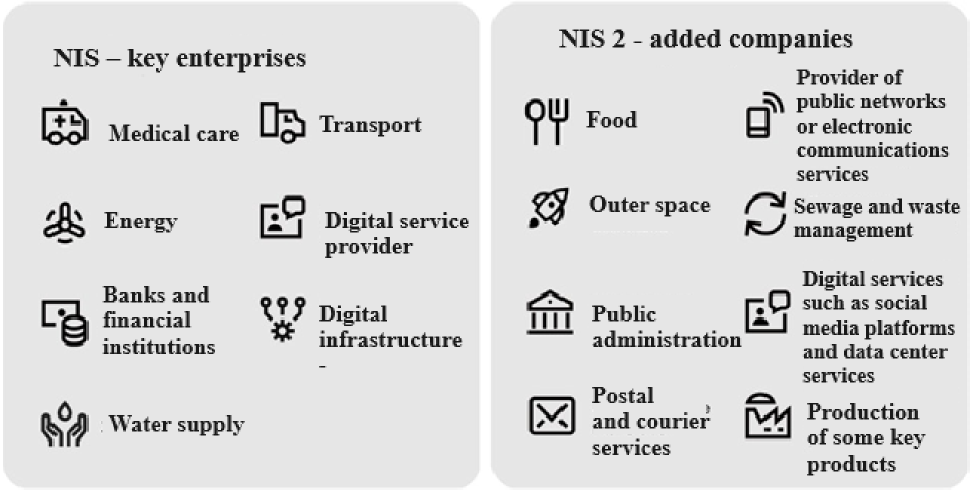
occurrence), (b) preventing the occurrence of incidents and attacks in the network of (EU and NATO countries), (c) improving cooperation between EU and NATO countries (exchange of information, implementation of best practices), and (d) strengthening the cyber resilience of EU and NATO countries.

The implementation of the aforementioned tasks is possible owing to appropriate legal, financial, planning, organisational, and technical conditions. Therefore, the first step that the EU took was to introduce the Directive on the Security of Network and Information Systems (NIS) in 2016, which concerned issues related to network infrastructure and IT systems. This document was the basis for the operation of many important enterprises such as medical care, transport, energy, digital service providers, banks and financial institutions, digital infrastructure, and water supply.[9]

The sharp increase in cyberattacks and incidents in Europe, as well as the identification of their negative impact on various areas of society, led to the introduction of Directive 2022/2555 of the European Parliament and Council on 14 December 2022 on measures for a high level of cybersecurity in the territory of the Union. This directive was repealed by the 2016 NIS Directive (NIS 1). The NIS 2 directive expanded the groups of enterprises to include food, public administration, space, providers of public networks or electronic communication services, postal and courier services, sewage and waste management, digital services such as social networking platforms and data centre services, and the production of key products (Figure 1).

[9] What is NIS2 and what does it mean for your organization? [Online]. Available at: https://www.nomios.pl/materialy/czym-jest-nis2/?utm_term=dyrektywa%20nis&utm_campaign=PL-PL+%7C+NIS2&utm_source=adwords&utm_medium=ppc&hsa_acc=5882528235&hsa_cam=21097975083&hsa_grp=163624375167&hsa_ad=693854520644&hsa_src=g&hsa_tgt=kwd-382086989990&hsa_kw=dyrektywa%20nis&hsa_mt=b&hsa_net=adwords&hsa_ver=3&gad_source=1&gclid=Cj0KCQjwltKxBhDMARIsAG8KnqWdbSCmaClWA9izjqe3UWZFyb5voEqHfqtYlPbsQHoVg9JxBRBEOscaAixGEALw_wcB. (Accessed: 30 March 2024).

Figure 1 *Comparison of key enterprises according to the NIS and NIS 2 Directives*


NIS – key enterprises
Medical care
Transport
Energy
Digital service provider
Banks and financial institutions
Digital infrastructure -
Water supply
NIS 2 - added companies
Food
Provider of public networks or electronic communications services
Outer space
Sewage and waste management
Public administration
Digital services such as social media platforms and data center services
Postal and courier services
Production of some key products

Source: Based on: What is NIS2 and what does it mean for your organisation? [Online]. Available at https://Czym jest NIS2 i co oznacza dla Twojej organizacji? Nomios Polska (Accessed: 30 August 2024).

For example, Poland has 8,000 entities in 18 economic sectors. The requirements of the NIS 2 directive also assume the development of more stringent procedures for reporting cyberattacks and incidents as well as increasing cooperation between EU countries in relation to responding to cyber incidents, exchanging information about them, and implementing the best and most effective practices. EU countries were obliged to implement it by 17 October 2024. In summary, the purpose of the new regulations was to create and implement a uniform standard for the security of network and information systems in all EU countries and to strengthen the Union's cyber resilience, taking into account Russia’s acts of aggression against Ukraine and its use of elements of cyber warfare.[10]

[10] NASK Cyber Policy, [Online]. Available at: https://cyberpolicy.nask.pl/aktualnosci/publikacja-dyrektywy-nis-2/ (Accessed: 30 April 2024).

2.1. Nato’s role in cyberspace

NATO has imposed certain solutions and regulations to ensure international security in cyberspace. Therefore, it is qualified using a steering subsystem. To implement the above-mentioned tasks, on 1 July 2012, the NATO[11] Cybersecurity Center (NCSC) was established based on the many years of experience of its predecessors (civilians and soldiers). It is located at the Headquarters of the NATO Allied Command in Europe (SHAPE) in Mons,[12] Belgium. The aim was to assist effectively in the coordination and cooperation in the management of cybersecurity information between NATO member states and their partners. It is an extensive platform aimed at (a) analysing and monitoring network incidents and attacks, (b) technical and expert support aimed at increasing cyber defence capabilities, (c) supporting member states in improving competencies, (d) developing the best regulation rights enabling the implementation of security policy in cyberspace, and (e) strengthening international cooperation (political consultation platform, joint actions).[13]

The NCSC employs approximately 3,000 civilian and military personnel who perform tasks at 34 locations in Europe and North America. It cooperates with sectors such as industry, scientific and academic communities, and non-profit organisations. These practices enable the maintenance of technological advantages.

NATO also established the Cyberspace Operations Centre in Mons, Belgium. This centre was established to support military commanders in allied operations and missions. It coordinates NATO's operational activities in cyberspace and indicates the cyber defence goals that must be implemented by the allied countries. These activities were conducted as part of the NATO defence-planning process. NATO also has the NATO Cyber Rapid Reaction Teams, which have 24/7 response capabilities; their main task is to help their allies. Additionally, NATO has its own international research and training centre, The NATO Cooperative Cyber Defense Center

[11] NATO Communications and Information Agency, [Online]. Available at: https://www.nato.int/cps/en/natohq/topics_78170.htm (Accessed: 23 April 2024).

[12] Supreme Headquarters Allied Power Europe, [Online]. Available at: https://shape.nato.int (Accessed: 23 April 2024).

[13] NATO Communications and Information Agency, [Online]. Available at: https://www.nato.int/cps/en/natohq/topics_78170.htm (Accessed: 23 April 2024).

of Excellence (CCDCOE) in Tallinn,[14] which aims to support member states and their partners in the field of cyber defence. NATO operations are governed by the provisions of Doctrine AJP-3.20, the Allied Joint Doctrine for Cyberspace Operations, This doctrine outlines key aspects of cyberspace operations, including their fundamental characteristics, as well as their planning and execution.[15]NATO has training and education facilities in the field of cyber defence at centres such as (a) The NATO Communications and Information (NCI) Academy in Oeiras, Portugal (training and education in the field of cyber defence); (b) The NATO School in Oberammergau, Germany (training and education in the field of cyber defence); and (c) The NATO Defense College in Rome, Italy (enabling the acquisition of skills in strategic thinking related to political and military issues, including cyber defence).

In summary, the management subsystem is strategic. The entities included in it are responsible for international security policies in cyberspace and, consequently, for cybersecurity, both in individual countries and in EU and NATO countries.

3. Assumptions of the cybernetic security system – the execution subsystem

The executive subsystem is crucial for every contractor, that is, the country. It consists of an operational sector (defence and protection) and a support sector (social and economic). The operational sector is crucial from the viewpoint of conducting activities aimed at preventing or responding to cyber-attacks or cyber incidents. The key role in the operational sector is played by the armed forces and, in the support sector, by society.

3.1. Armed conflicts and cyberspace

While analysing various armed conflicts, it should be emphasised that in addition to standard activities, propaganda, information, and media activities were also used. Therefore, the terms ‘media war’ and ‘propaganda war’

[14] The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary cyber defence hub, [Online]. Available at: https://ccdcoe.org (Accessed: 23 April 2024).

[15] Allied Joint Publication-3.20, Allied Joint Doctrine for Cyberspace Operations, [Online]. Available at: https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf (Accessed: 30 August 2024).

were used to describe some conflicts. Such wars were as follows: (a) the Iran–Iraq War (1980–1988),[16] (b) the Persian Gulf War (1990–1991),[17] (c) the Iraq War (2003–2011),[18] (d) the war against ISIS (2014–2017),[19] and (e) the war with Russia (2018–2019). These wars were mainly based on propaganda, information, and media. The Vietnam War (1955–1975) was the first to have a significant presence in the media.[20]

The participants in the conflict were politicians who provoked the war, soldiers taking part in it, and the media, in that order. The most important conclusion from this conflict in relation to the strategy of military operations was the statement that 'in order to conduct foreign policy, it is necessary to control the information that the media transmit to the public',[21] which is why, from a political and military viewpoint, it is so important to control the information transmitted to the public. The media had access to it during the Vietnam War. This situation changed after the government, politicians, and commanders realised the media's influence on armed conflicts. In several subsequent conflicts, they were not allowed to report events.

Currently, the media are treated as partners under certain rules. Journalists focus on providing information about the winning side of the conflict, and in many cases, any information intended to reach the public is censored by the government and military sectors. These assumptions have brought great success to the American government. The media effectively influenced Americans' opinions, which were shaped by controlled media coverage. In summary, the role of the media is to create appropriately directed images to influence public opinion.

The Iran–Iraq War was an armed conflict that lasted from 1980 to 1988. Over one million people died during this war, and material losses

[16] Iran-Iraq War, [Online]. Available at: https://www.history.com/topics/middle-east/iran-iraq-war (Accessed: 10 April 2024).

[17] Persian Gulf War, [Online]. Available at: https://www.history.com/topics/middle-east/persian-gulf-war (Accessed: 10 April 2024).

[18] The Iraq War, [Online]. Available at: https://www.georgewbushlibrary.gov/research/topic-guides/the-iraq-war (Accessed: 10 April 2024).

[19] The Conflict with ISIS: Operation INHERENT RESOLVE, June 2014–January 2020, [Online]. Available at: https://history.army.mil/html/books/078/78-2/index.html (Accessed: 10 April 2024).

[20] The Conflict in Iraq and the media (media manipulation, or how beneficial it is sell your strategy), [Online]. Available at: mak00 (uw.edu.pl) (Accessed: 30 April 2024).

[21] Ibid.

were estimated to be over USD 400 billion.[22] This conflict is believed to have caused the greatest losses in the 20th century. The main strategy was military operations on the front, but propaganda activities were also used to influence public opinion both inside and outside the country. It was the first war in which both sides manipulated information to gain support from each other and weaken the opposing side. These activities focused on presenting images from the battlefield and reporting them, as well as broadcasting propaganda messages from leaders. These goals were achieved through radio, television, printed materials, the Internet, and emerging media. Both Iraq and Iran had control over radio and television stations and the content published in articles and images was distributed to the public. Both sides use posters and leaflets depicting war heroes, patriotic slogans, and national flags. This aimed to encourage society to fight and think about it in terms of necessity. Although the Internet and media were still scarcely used at that time, activities were also undertaken to promote specific information, including photos and films depicting the course of the war and specific situations intended to influence public opinion.

The Iran–Iraq War is an example of the possibility of having a strong impact on society through the use of disinformation or propaganda.

Another example of media warfare was the Persian Gulf War (1990–1991). All parties involved in the conflict conducted propaganda and information activities. This war was reported on an ongoing basis. Journalists tried to provide reliable and current information, but this was hindered by the authorities, who wanted to promote an appropriately created message. Journalists had access only to selected combat zones or certain events, and the military often decided what was to be published. Interest among journalists was very high: 3,000 people from all over the world volunteered to cover the war. However, only 600 journalists were given access to the clash sites, 500 of whom were Americans.[23] A rule was also adopted in which journalists were assigned to military units to limit their freedom of action. The interests of the independent journalists were not those of either side of the conflict. The government wanted to provide the public with information aimed at confirming their belief in the right to wage

[22] Iran-Iraq War, [Online]. Available at: The Iran-Iraq War - (bing.com) (Accessed: 30 April 2024) and Wideo The Iran-Iraq War, [Online]. Available at: Iran-Iraq War - Summary, Timeline & Legacy (history.com) (Accessed: 20 April 2024).

[23] The Conflict in Iraq and the media (media manipulation, or how beneficial it is selling your strategy) [Online]. Available at: mak00 (uw.edu.pl) (Accessed: 30 April 2024).

armed conflict. Despite these restrictions, journalists tried, often risking their own lives, to reach the frontline. Manipulation and propaganda have become variants of action on both sides. Thanks to media activities, information about the war in the Persian Gulf spread widely and sparked a global discussion on the legitimacy of war, its ethics, foreign policy, and international security. Widely discussed war has stimulated public discussion worldwide.

Another example of a media war was the war in Iraq (2003–2011), which was initiated by the United States under the pretext that Iraq possessed weapons of mass destruction (chemical and biological weapons and ongoing nuclear weapons development) and connections with terrorist organisations. During the war, photos and films were manipulated in such a way that military actions were perceived positively and enemy actions were perceived negatively. Both sides of the conflict controlled media messages. Journalists were given limited access to the areas where the war was taking place, and the content appearing in the press was censored by state media. Saddam Hussein's administration organised and carried out information and propaganda campaigns aimed at creating a positive image of the regime and condemning military invasions. Both sides promoted their own narratives to create positive images of their actions, events, and interests. The manipulation was performed using appropriately selected words, phrases, or sentences.

Another example of the use of information and propaganda activities is the war against ISIS (2014–2017). The Islamic State (a terrorist group) has extensive and well-functioning propaganda cells. The main goal was conscious or unconscious beliefs about the ideas being promoted. ISIS conducts propaganda activities in cyberspace and is characterised by a high level of technology. These tactics are intended to gain the interest of recipients and recruit them to join the organisation. Messages in the form of photos and videos, based on various social media platforms, such as Facebook and Twitter, are created with utmost care and use the latest technologies. The Internet and social media have become cheap channels of access to society worldwide, facilitating the coordination of tasks within a group, enabling real-time reporting of actions taken, and conducting propaganda activities. The State of Islam conducts large-scale information activities, trying to intimidate society and recruit new supporters of the "soldiers" ready to arrive at their areas or carry out activities as 'lone wolves'. Online activities also include the use of cryptocurrencies for terrorist activities, the flow of which is much more difficult to detect than in traditional financial funds. Because of this solution, financing the activities of criminal organisations has become easier. Social networking sites were also used for these activities. Fictitious profiles were created, and Israeli soldiers were contacted to gain access to information about the army's activities and the prevailing mood among soldiers and society.[24]

An effective tool for propaganda and disinformation is fake news, which is partially or completely false information intended to mislead the recipient to achieve financial, political, ideological, and prestigious benefits. Research shows that false, often negative, information spreads much faster than true, often positive, information.[25] Learning how society functions makes it easier to organise activities that have an expected impact on the recipient.

Propaganda activities were also conducted by the Russian Federation (2018–2019) in all possible information areas using the media. They provided information, disinformation, propaganda, and psychological operations. To achieve these goals, an extensive information apparatus was used, which included leaders, commanders, journalists, and special services. Russia used all available means to create content in cyberspace. The created content included portraying the policies of the United States and NATO countries negatively, depreciating Poland’s defence capabilities, and shaping the negative image of the European Union and Ukraine. Russia constantly conducts information warfare in cyberspace to pursue its own interests. Russia is a brutal player in the international arena and is famous for its disinformation campaigns using false accounts on social media. These activities are usually aimed at democratic countries and their alliances. Their strategic goal is to weaken countries and alliances that condemn Russia’s actions, as well as to promote Russia as a great power. Russia has used various means to achieve these goals. One of them is engaging in cyber warfare. They have well-trained hacker groups that attack political, economic, military, and other economic goals. Their main goals are to steal sensitive data, spy on strategic areas, and sabotage IT and

[24] Information Warfare as a Contemporary Tool of Irregular Operations, [Online]. Available at: Wojna_informacyjna_jako_współczesne.pdf (Accessed: 30 April 2024).

[25] Study: On Twitter, false news travels faster than true stories Research project find humans, not bots, are primarily responsible for spread of misleading information, [Online]. Available at: https://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308 (Accessed: 30 April 2024).

information systems, critical infrastructure, and other facilities crucial to the state's defence. Russia is suspected of interfering with elections in various European Union countries as well as in the United States through the use of social media, the Internet, and websites. The main goal of these actions was to weaken the country's position while simultaneously strengthening Russia's influence.

In summary, cyberspace has become a completely new and modern platform for conflict. In the literature, it was swiftly recognized as an additional arena of warfare, alongside land, sea, and air. This domain is, on the one hand, very challenging, and on the other hand, a remarkably accessible platform for waging war. Information has become a commodity because it is easily accessible. Anyone with basic knowledge of how to use computer hardware or software can create events, cause panic and chaos in societies, and influence the opinions of users. It is difficult to detect fake accounts and information inserted into a network, and this requires the involvement of many people or even extensive structures dedicated to such tasks.

Conflict in cyberspace has become a reality. In 1991, after the Persian Gulf War, one of the conclusions was that information could be freely presented on the Internet; therefore, it was very important to control the messages being shared. This belief was further strengthened by research conducted among the American community in 1991, which revealed that as much as 89% of knowledge about the Persian Gulf War was obtained from television, and only a few citizens assessed the course of this war through the prism of experience.[26] This demonstrates the powerful tools of propaganda and disinformation, especially when used in cyberspace. Due to these tools, it is possible to create a societal perception of conflict in various countries and, thus, influence the policy of a given nation or the world.

3.2 Armed forces in cyberspace

Information protection is a basic task for every country's armed forces. In the activities of the armies of nations, it is important to maintain the confidentiality of military information, the effectiveness of its transmission, and its quality and credibility. This is made possible through information protection, during which the following actions are taken: counterintelligence, technical security of IT infrastructure, IT protection,

[26] The Conflict in Iraq and the media (media manipulation, or how beneficial it is selling your strategy), [Online]. Available at: mak00 (uw.edu.pl) (Accessed: 30 April 2024).

engineering development aimed at anticipating the enemy's actions, psychological protection, counter-disinformation, and reconnaissance (deterring and incapacitating the enemy). Information protection involves securing information in such a way as to prevent undesirable disclosure, modification, or destruction. Defensive actions are being taken to protect the so-called sources of information or information environment shields. Information protection is thus strategically important for security systems, as any loss or disruption may weaken the information battlefield.

Defence potential focuses on the armed forces, which also carry out tasks related to security in cyberspace. Next to land, water, and air, cyberspace has become another area of warfare (for the armed forces) and is important from the perspective of the strategic, defence, and protective capabilities of the armed forces. In this space, cyberattacks are prevented, information is collected, and defence is implemented. It is also a place where the communication and coordination of operations, missions, and tasks are conducted. The main tasks of the armed forces in cyberspace are (a) protection of IT infrastructure (equipment and networks, as well as systems dedicated to specific tasks), sensitive data, and information contained therein; (b) data collection (e.g. monitoring the enemy's activities, its capabilities and intentions to act); (c) conducting intelligence activities (open and closed sources); (d) coordinating activities (possible at all levels of command); (e) counteracting cyberattacks and conducting offensive activities (implemented through a cyberattack on the enemy's infrastructure, information espionage, information warfare, propaganda, strategic communication, operational information, psychological operations, disinformation, sabotage of enemy systems, information manipulation); (f) communication (possible between team members, carried out using secure channels); (g) professional development (possibility of training soldiers and civilian staff in the field of cybersecurity, conducting exercises and simulations based on real scenarios); and (h) technological scientific development (conducting work on artificial intelligence, cryptology, cybersecurity technologies, big data).

Nowadays, thanks to modern technologies, the problem is not access to data, but access to too many differently formatted data. In this context, 'big data' are particularly noteworthy. Big data refers to four important Vs: (a) volume (processing large amounts of data); (b) velocity (data generated at high data transfer speeds); (c) variety (different types of data); and (d) veracity.[27]. Owing to big data analyses, it is possible to detect potential cyberattacks and cyber criminals, making real-time analysis, which is important for an effective and immediate response to incidents, preventing DDoS attacks, and protecting personal data and sensitive, official, and classified information.

Ensuring the safety of citizens and the nation requires the involvement of many forces and resources, as well as strategies and variants of action. Rapid technological development has become a fundamental factor in shaping the world and its functioning in all areas. This also applies to safety concerns. Achieving satisfactory security in a country depends on several factors. Therefore, various operational strategies and methods have often been combined. Multidirectional and diverse methods contribute to greater effectiveness than their individual uses. Anyone is responsible for safety, which is why the attitude of every person and citizen is important. This attitude depends on external factors such as the available information provided by various means of communication. On this basis, opinions and social attitudes are built and, consequently, actions are taken. Therefore, various, often very aggressive, actions shape public opinion not only in the country but also abroad. To achieve these assumptions, the following instruments can be used: propaganda, information warfare, disinformation, psychology, information, propaganda, and military disinformation operations.[28] These actions are intentional and allow the achievement of assumed political and military goals.

Psychological operations are carefully planned operations aimed at transmitting selected information to foreign recipients to induce specific emotions, motivations, and, ultimately, specific behaviours of foreign governments, institutions, or citizens. The assumption of the aforementioned operations is to obtain behaviour conducive to a nation’s goals. This is part of not only diplomatic, informational, and economic activities but also military ones. They are used in times of crisis and armed conflict.

[27] Big Data Analytics, [Online]. Available at: https://www.cybertec-postgresql.com/pl/data-science/analityka-big-data/?gad_source=1&gclid=CjwKCAjwxLKxBhA7EiwAXO0R0AP4wteDaJk5guP13G2Q2b9aDMXLecz9C3UVW1Dj0y0w2GovF2HTyhoCaOcQAvD_BwE (Accessed: 15 February 2024).

[28] *Disinformation and Propaganda in the Context of Threats to State Security, Review of Constitutional Law, [Online].* Available at: Dezinformacja i propaganda w kontekście zagrożeń dla bezpieczeństwa państwa - Przegląd Prawa Konstytucyjnego - Issue 2(24) (2015) - CEJSH - Yadda (icm.edu.pl) (Accessed: 11 February 2024).

Psychological operations are carried out at the strategic, operational, and tactical levels. They may negatively impact soldiers' morale, reduce the enemy's ability to conduct or sustain military operations and attract attention. [29]

Information operations are the integrated implementation of projects aimed at influencing the attitudes of commanders and those in power, disrupting the functioning of IT systems and data carriers or destroying them, and corrupting decision makers while protecting one's own information and the systems processing it. Information operations are divided into offensive (OIO) and defensive (DIO) operations. OIA include intelligence-supported capabilities and activities. They influence the opponent's decisions and promote specific planned goals, that is, activities aimed at attacking information about the opponent and everything related to him. Defensive operations aim to protect information and IT systems. [30]

Propaganda operations are defined as (a) planned and purposeful activities aimed at shaping specific views and behaviours of society based on directed images, slogans and symbols referring to human prejudices and emotions[31]; (b) planned and purposeful, skilful use of communicating a certain viewpoint, aimed at persuading the recipient to voluntarily recognise this point of view as their own, (c) activities aimed at 'intentional dissemination of information, opinions, views, theories explaining the surrounding reality and phenomena of social life'; (d) activities using the technique of influencing behaviour of citizens, managing and manipulating public opinion. These activities can be improved based on research results, among others, in the fields of social psychology, sociology, political science, and communication theory.

The assumption behind this type of activity is that government authorities lie to societies. A lie can be directed at an opponent, international

[29] Psychological Operation, [Online]. Available at: https://www.globalsecurity.org/military/library/policy/usaf/afdd/2-5-3/afdd2-5-3.pdf; (Accessed: 11 February 2024) and Department of Defense Dictionary of Military and Associated Terms, [Online]. Available at: https://irp.fas.org/doddir/dod/jp1_02.pdf (Accessed: 3 February 2024).

[30] Vademecum of Information Security. Information Operations, [Online]. Available at: https://vademecumbezpieczenstwainformacyjnego.uken.krakow.pl/2020/03/11/operacje-informacyjne/ (Accessed: 13 February 2024).

[31] Vademecum of Information Security. Propaganda operations, [Online]. Available at: https://vademecumbezpieczenstwainformacyjnego.uken.krakow.pl/2020/03/11/operacje-propagandowe/ (Accessed: 12 February 2024).

opinion, or society. These activities focus on deliberate and planned intellectual and emotional manipulations carried out using false arguments, which should be considered disinformation. Propaganda aims to convince the recipient to accept content directed by the authorities in a country or countries or, based on it, to change awareness and beliefs about matters that are important in the country. Propaganda is also understood as persistent teaching. It is associated with terms such as lying, brainwashing, propagating slogans, speaking against someone or something, politicisation, and indoctrination. Propaganda uses many techniques to reach a recipient (e.g. image, sound, body language, written text, film, theatre, dance, radio, television, and social media). Broadly, propaganda refers to emotions rather than reason.[32]

The literature provides various types of propaganda. When it comes to defining intentions and sources, the following are distinguished: (a) white propaganda (intentions and sources open), (b) grey propaganda (intentions and sources unclear and open), and (c) black propaganda (intentions, hostile, enemy-oriented sources).[33]

There is also propaganda that is (a) political (influencing the opinion of society; used by governments, political parties, interest groups), (b) advertising (promoting products or services; used by entrepreneurs), (c) military (mobilising support for a specific side, demonising the enemy, increasing morale among soldiers and civilians; used by authorities, commanders), (d) religious (promoting faith, attracting followers; used by churches, religious organisations), (e) racial/ethnic (goal beliefs about the advantage of one group or race; used by governments, social groups), (f) health (goal belief in changing health behaviours; used by health services, government), (g) cultural (goal promoting cultural values; used by the government, specific organisations), (h) social media (goal spreading disinformation, manipulating public opinion, influencing elections; used by the government, specific social groups),[34] (i) state (goal promoting patriotism, justifying government policy; used by government, specific groups), and (j) corporate (goal promoting corporate interests; used by companies).

[32] Dobek-Ostrowska, Fras and Ociepka, 1999.

[33] Vademecum of Information Security. Propaganda operations, [Online]. Available at: https://vademecumbezpieczenstwainformacyjnego.uken.krakow.pl/2020/03/11/operacje-propagandowe/ (Accessed: 15 February 2024).

[34] Batorowska, Klepka, and Wasiuta, 2019.

Military disinformation operations are defined as pre-planned activities that are part of military operation plans. Their goal is to mislead the opposing side regarding their own activities, namely, the number of forces at their disposal, their location, and combat readiness. This is intended to influence the opponent's decisions. The effects of this type of operation are as follows: chaos caused by the information received and favourable behaviour of the opponent in relation to his own side (inappropriate allocation of forces and resources to the task being carried out, unmasking the strengths and weaknesses of the opponent, revealing the intentions and intentions of action, and loss of combat capabilities).[35] Military disinformation operations are extremely difficult; therefore, they require a special focus on issues such as the purpose of the action (causing the enemy to take specific actions), security, timeliness (determining the most favourable time to carry out the operation), planning and control (implemented by the central command), and integration (coordination of activities with the operations that support them). [36]

3.3. Organisation of cybersecurity in the Republic of Poland

The NIS Directive imposed the same solutions on all European Union countries in the field of information protection as part of cyberspace security. In relation to its provisions, the following have been established in Poland: (a) the National Computer Security Incident Response Team run by the Ministry of National Defense, operating as part of the Cyberspace Defense Component Command (CSIRT) of the Ministry of National Defense;[37] (b) the Computer Security Incident Response Team, national level, led by the Head of the Internal Security Agency (SIRT GOV);[38] and (c) the Computer Security Incident Response Team, national level, led by the Scientific and Academic Computer Network (CSIRT NASK).[39] Their

[35] Kacała, 2015.

[36] Vademecum of Information Security. Military Disinformation Operations, [Online]. Available at: https://vademecumbezpieczenstwainformacyjnego.uken.krakow.pl/2020/03/11/operacje-wojskowej-dezinformacji/(Accessed: 10 February 2024).

[37] Cyberspace Defense Forces, [Online]. Accessed at: https://www.wojsko-polskie.pl/woc/(Accessed: 20 February 2024).

[38] Computer Security Incident Response Team, [Online]. Available at: https://csirt.gov.pl (Accessed: 10 February 2024).

[39] Day-To-Day Activities of the Computer Security Incident Response Team Under the Act on the National Cybersecurity System, [Online]. Available at:

tasks include (a) monitoring cyber incidents and cyber threats; (b) risk analysis in connection with disclosed cyber threats or cyber incidents; (c) exchanging information between authorised entities; (d) responding to cyber-attacks or cyber incidents; (e) issuing announcements about identified cyber threats or cyber incidents; (f) classifying incidents; and (g) conducting analyses, research, and development in the field of cybersecurity[40]

In the Republic of Poland, the provision that responds to the implementation of the NIS directive is primarily the Act on the National Cybersecurity System, which was adopted on 5 July 2018. According to its provisions, the entities included in the above-mentioned system are (a) key service operators, (b) digital service providers, (c) CSIRT MON, (d) CSIRT NASK, (e) CSIRT GOV, (f) sector teams cybersecurity, (g) public finance sector entities, (h) research institutes, (i) National Bank of Poland, (j) Office of Technical Inspection, (k) Polish Air Navigation Services Agency, (l) Polish Center Accreditation, (m) National Fund for Environmental Protection and Water Management and provincial funds for environmental protection and water management, (n) commercial law companies performing public utility tasks, (o) entities providing cybersecurity services, (p) authorities competent for cybersecurity, (r) Single Contact Point for cybersecurity, (s) Government Plenipotentiary for Cybersecurity, and (t) Cybersecurity College.[41]

The Act also covers the Cybersecurity Strategy of the Republic of Poland, which was adopted in 2019 by the Council of Ministers for 2019–2024, which implements five specific objectives of the government's policy: (a) development of the national cybersecurity system; (b) increasing the level of resilience of public administration and sector information systems, and achieving the ability to effectively prevent and respond to incidents; (c) increase the national potential in the field of cybersecurity; (d) build awareness and social competencies in the field of cybersecurity; and (e) build a strong international position in the Republic of Poland in the area of

https://www.nask.pl/pl/projekty-dofinansowane/projekty-realizowane-ze/3959,Dzialalnosc-biezaca-Zespolu-Reagowania-na-Incydenty-Bezpieczenstwa-Komputerowego.html (Accessed: 10 February 2024).

[40] CSIRT of the Ministry of National Defence, [Online]. Available at:https://csirt-mon.wp.mil.pl/pl/pages/zadania-2017-01-16-4/ (Accessed: 15 February 2024)

[41] National cybersecurity system, [Online]. Available at: https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/krajowy-system-cyberbezpieczenstwa-18746756 (Accessed: 15 February 2024)

cybersecurity. [42] It is also worth mentioning the doctrinal document ratifying the doctrine of AJP 3.20, Operations in Cyberspace. Professor Piotr Dela is a recognised expert in the field of cybersecurity, with works on topics such as elements of the combat system in cyberspace,[43] the theory of combat in cyberspace,[44] and assumptions of operations in cyberspace,[45] as is Dr. Robert Janczewski.[46]

3.4. Social potential of cybersecurity

According to the author and other experts, the social potential of cybersecurity is conditioned by the awareness of every citizen regarding threats to cyberspace and the related consequences. Educational, scientific, and technological developments have a significant impact on the development of cyberspace. Society plays a significant role in this respect if it is highly qualified and competent in the field of contemporary threats and security challenges, and constitutes invaluable social capital, thanks to which it is possible to ensure social development and, consequently, high quality of life and security of citizens.

The security of the state also depends on every citizen; therefore, awareness, knowledge, and skills in the field of cyber incidents that may occur or have already occurred are necessary. This can be achieved through an education system, awareness, application of security procedures, safe use of the Internet, activities in initiatives related to cybersecurity, reporting of cyber incidents, and civic initiatives (action within the community).

According to the author and experts, cybersecurity education should be implemented systematically to include several elements. The first are the curricula at the kindergarten, primary school, secondary school, and university levels, which should complement each other. The content should be age appropriate and cover issues such as online threats, basic rules for the safe use of the Internet, and rules for protecting private data. Along with the knowledge of these threats, it is necessary to focus on recognising them and applying an algorithm to deal with emerging cyber incidents.

[42] Cybersecurity strategy of the Republic of Poland for 2019-2024, [Online]. Available at: https://cyberpolicy.nask.pl/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024/(Accessed: 22 February 2024).

[43] Dela, 2020b.

[44] Dela, 2020a.

[45] Dela, 2022.

[46] Janczewski, 2023.

At the student level, topics such as cryptography, information security, information society, IT security, detection of attacks on computer systems, security of computer systems, cyberdefence,[47] and cyber risk management should be included. In addition to exploring and improving their knowledge in the abovementioned areas, students should be able to conduct research in the field of cybersecurity and popularise their results on their own or together with their professors. Another element is the training and workshops in the military, non-military, and social sectors dedicated to working or serving society. The elements supporting the above measures are e-learning platforms containing training materials in the fields of cybersecurity, scientific research, technology development, and social incentives, although these should be classified as activities that signal the issue of cybersecurity.

An appropriate education system will contribute to increasing awareness of the consequences of threats in cyberspace, which will make citizens (a) capable of functioning in cyberspace using proven security practices such as setting strong passwords, updating software, ignoring suspicious links and attachments, and using anti-virus software; (b) use the Internet responsibly by not sharing personal data, private photos, and videos of themselves and their family members; material goods; checking their bank accounts; and monitoring transactions; (c) avoid participating in illegal activities on the Internet; (d) promote and popularise knowledge about safe functioning on the Internet; (e) report cyber incidents promptly; and (f) be careful when using public Wi-Fi networks.

Nowadays, in the face of many aggressive threats in cyberspace, citizens must have knowledge of them, as well as skills in using digital technologies and initiating security procedures. These factors will have a significant impact on ensuring the safety of individuals and the immediate environment, while also contributing to the broader goal of national security as part of a citizen's responsibility.

4. Conclusions

This analysis of the literature on the subject, reports, Internet sources, and interviews with experts allows us to conclude that cyberspace is a friendly environment in which various processes can take place. Therefore, this issue

[47] Cyber defence, [Online]. Available at: https://www.nato.int/cps/en/natohq/topics_78170.htm (Accessed: 23 April 2024).

should be considered comprehensively, in a systemic way, considering all the features associated with the term ‘system’. It is vital to clearly indicate who is responsible for creating the cybersecurity policy, its strategy, and methods of implementation, as well as the entities responsible for employing the policy. With the dynamic technological developments, the security of cyberspace and society is changing. Currently, it is necessary to constantly recognise all current and potential threats and urgently and systematically introduce changes to legal provisions and procedures that will provide formal and practical opportunities to build cyber defence in individual countries and, consequently, in the structures of NATO and the EU.

In summary, the author of this article assumes that the cybersecurity system is a set of forces and resources understood as personal and material resources allocated by the state or states to implement tasks related to security in cyberspace. This system distinguishes between management and executive subsystems, consisting of the operational sector (security and defence) and the support sector (socioeconomic). It was also assumed that from the perspective of carrying out activities aimed at preventing or responding to cyberattacks or cyber incidents, the armed forces play a key role in the operational sector and society in the support sector.

Bibliography

[1] Batorowska, H., Klepka, R., Wasiuta, O. (2019) *Media as an Instrument of Information Influence and Manipulation of Society.* Kraków: Libron.

[2] Dela, P. (2020a) *Theory of combat in cyberspace.* Warsaw: Warsaw Academy of Art Publishing House.

[3] Dela, P. (2020b) 'Elements of the combat system in cyberspace', *The Bellona Quarterly,* 2020/3, pp. 69-84; https://doi.org/10.5604/01.3001.0014.6161.

[4] Dela, P. (2022) A*ssumptions in cyberspace*. Warsaw: PWN Scientific Publishing House.

[5] Dobek-Ostrowska, B., Fras, J., Ociepka, B. (1999) *Theory and Practice of Propaganda.* Wroclaw: Publishing House of the University of Wrocław.

[6] Janczewsk, R. (2023) *Cyberfight. Military dimension of operations*. Warsaw: PWN Scientific Publishing House.

[7] Kacała, T. (2015) 'Disinformation and Propaganda in the Context of Threats to National Security', *Przegląd Prawa Konstytucyjnego,* 24(2), pp. 49 - 65; https://doi.org/10.15804/ppk.2015.02.03.

[8] Wiśniewski, B. (2013) *State security system. Theoretical and practical contexts*. Warsaw: PWN.