FOUR AREAS OF CYBERSECURITY – DISCUSSION OF THE SUBJECT AREA

Cybersecurity involves not only ensuring security for the functioning of infrastructure, devices and electronic equipment, but also the protection of information and data on the Internet. We are more or less aware of how to take care of the material goods, such as the transmitters, servers, etc., but we do not fully understand the Internet environment, i.e. cyberspace, where the content we want to protect is located. At the same time, the concepts of crime and hybrid war are expanding, having effects both in the physical and virtual world. Cybersecurity is a challenge to hybrid threats.

The definition of cybersecurity covers four areas that should be discussed as one group:
1. cyberspace law,
2. security systems and institutions responsible for cybersecurity,
3. the Internet as a media environment,
4. the Internet as a new social environment.

It is impossible to create a coherent security system in cyberspace if for some reason one of the presented areas is not taken into consideration.

Area 1. Cyberspace law

There is no commonly accepted definition of cyberspace. So far, attempts to define this concept are of a general nature. Cezary Banasiński writes: “In both broad and abstract terms, cyberspace is a global information infrastructure, mutual communication between people using computers and telecommunication, a communication space created by a system of Internet connections that enables the network user to make real-time contacts and covers all electronic communication systems that send information from numerous sources” or “the worldwide information domain, where the electromagnetic spectrum is a data carrier”, and “the space of open communication via connected computers and IT memories working all over the world”.

---

1 Slawomir Stalmach – expert in information security analysis at the Academic Centre for Cybersecurity Policy at War Studies Academy, also writing a PhD dissertation in sociology at Collegium Civitas in Warsaw. 

Correspondence address: <s.stalmach@akademia.mil.pl>.

Polish law penalises many crimes in cyberspace, including theft, forgery, destruction, fraud, incitement to criminal activities, stalking, etc. In 2014, Poland ratified the Council of Europe Convention on Cybercrime\(^3\). Many provisions on crime related to networks and computers have been introduced to Polish law, mainly to the Criminal Code. For instance, Article 267(1) of the Criminal Code provides: “Whoever, without being authorised to do so, acquires information not destined for him, by opening a sealed letter, or connecting to a wire that transmits information or by breaching electronic, magnetic or other special protection for that information shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to 2 years”\(^4\).

The reality is always ahead of the legislation, especially when we are discussing the dynamically developing Internet space. There are also new types of law violation, which are now mostly used in English, such as: sniffing, \textit{i.e.} data interception; spoofing, \textit{i.e.} posing as another element of the IT system; phishing, \textit{i.e.} stealing confidential data, and others\(^5\). Piotr Kardas states that: “With the increase of the number of entities having access to cyber systems that collect and process information, which are currently symbolised by the Internet network, which allows almost everyone to have access to information and the possibility of creatively shaping it, there is an increasing number of areas for potential conflicts derived from access to information sources, as well as the possibility of using them and influencing their shape”\(^6\).

**Definition of cybersecurity in Polish law**

Katarzyna Chałubińska-Jentkiewicz points out that legal regulations on cybersecurity in Poland are not gathered as a whole: “It should be emphasised that the legal regulations that today can be classified as those for cybersecurity are very often dispersed, covering very different areas of life. The above problem has not been solved by the Act of 5 July 2018 on the National Cybersecurity System”\(^7\).

Despite these reservations, it should be noted that in the Act on the National Cybersecurity System, cybersecurity is defined as: “Resistance of information systems to activities violating the confidentiality, integrity,
availability and authenticity of the processed data or related services offered by these systems."

The Cybersecurity Strategy of the Republic of Poland for 2019–2024 was adopted almost at the same time as the Act on the National Cybersecurity System. The strategy was described by Marek Zagórski, Minister of Digital Affairs: “The adoption of the Act on the National Cybersecurity System in 2018 created the legal and organisational foundations for building, for the first time in history, a comprehensive cybersecurity system in Poland. This system will be constantly developed, which was clearly pointed out in one of the detailed objectives for the Strategy. Moreover, the priorities in the area of information security for the Polish government were indicated”.

Next, in the National Security Strategy of the Republic of Poland, which was adopted in May 2020, cybersecurity was highlighted in the first pillar, which describes the security of the state and citizens. Cybersecurity was intentionally placed between the regulations on the armed forces of the Republic of Poland and the information domain, which indicates their inseparable relationship. “In the context of the digital revolution, the specific role of cyberspace and information space should be taken into account”.

The specific tasks included in the National Security Strategy related to the sphere of cybersecurity are as follows:

“4. Increasing resilience to cyber threats and boosting information protection in the public, military and private sectors as well as fostering knowledge and good practices enabling citizens to better protect their information:

4.1 Increasing resilience in the public and private, as well as in the military and civilian information systems, and attaining the capability to effectively prevent, combat and respond to cyber threats.

4.2 Strengthening the defensive capabilities of the state by ensuring continuous development of the national cyber security system.

4.3 Attaining capabilities to conduct full spectrum of military operations in cyberspace.

4.4 Developing national capabilities in the area of testing, research, assessment and certification of cyber security solutions and services.

---

8 Act of 5 July 2018 on state cybersecurity system [Dz.U., 2018, item 1560, Article 2(4)].
10 Ibid., p. 2.
4.5 Developing competences, knowledge and awareness of threats and challenges among public administration employees and in the society, in the domain of cyber security.

4.6 Strengthening and developing national potential, *inter alia*, through development of domestic solutions in the area of cyber security and by conducting state-funded research and development work in the domain of modern technologies, among others, machine learning, the Internet of Things, fixed-line and mobile broadband networks (5G and subsequent generations), including cooperation with universities, scientific institutions and enterprises from both public and private sectors”\textsuperscript{12}.

Furthermore, specific tasks related to the information space described in the Strategy are:

“5. Ensuring secure functioning of the state and its citizens in the information space:

5.1 At the strategic level, building capabilities to protect the information space (including systemic fight against disinformation) understood as the merging layers of space: virtual (the layer of systems, software and applications), physical (infrastructure and equipment) and cognitive.

5.2 Creating a homogenous system of strategic communication of the state, whose task should consist in forecasting, planning and implementing coherent communication activities, using a wide range of communication channels and media, and applying identification and influence tools in various domains of national security.

5.3 Actively counteracting disinformation by building capabilities and creating procedures defining cooperation with the information and social media while ensuring the involvement of citizens and non-governmental organisations.

5.4 Aiming to increase public awareness of threats related to the manipulation of information through education in the field of information security”\textsuperscript{13}.

Finally, an obvious recommendation from the National Security Strategy: “The provisions of this document should be further extended and reflected in national strategic documents pertaining to national security and development of Poland”\textsuperscript{14}.

**Area 2. Security system and institutions responsible for cybersecurity**

The most important notions that define the national cybersecurity system are: critical infrastructure, key digital services and the manner of responding to so-called computer security incidents.

The security system in our country provides the protection of infrastructure including communication systems and ICT networks, because these are resources that are essential for the safe functioning of the

\textsuperscript{12} Ibid., p. 20.

\textsuperscript{13} Ibid., p. 21.

\textsuperscript{14} Ibid., p. 5.
economy and society. In this context, one may discuss so-called critical infrastructure, i.e. facilities, devices, installations and systems. Art. 3.2 of the Crisis Management Act defines what should be recognised as critical infrastructure, so these are: “(...) systems and mutually bound functional facilities contained therein, including constructions, equipment, installations and services of key importance to the security of the state and its citizens as well as serving to ensure the efficient functioning of public administration authorities, institutions and enterprises”\(^\text{15}\).

The Act on the National Cybersecurity System of 2018 introduces the concept of key digital services and their operators\(^\text{16}\).

Operators are entities (both companies and public institutions) that:
— provide key services,
— the delivery of these services depends on information systems,
— an incident in these entities had a significant disruptive effect on the delivery of the service.

Operators are also entities that run business in transport, road management, mineral extraction, electricity generation, transmission and distribution, energy infrastructure management, heat generation and transmission, storage and transmission of liquid and gaseous fuels, trade and distribution of medical products, banking and financial market infrastructure, and digital services delivery. The full spectrum of key services is enlisted in the regulation of the Council of Ministers of September 11, 2018\(^\text{17}\).

Another very important concept for the cyberspace security system is the definition of a computer security incident and what institutions are obliged to react to the incident. Generally, in this aspect, it is defined as: “An incident is an action that poses or may pose an unfavourable impact on cybersecurity”\(^\text{18}\). The so-called incident handling includes: “activities enabling detection, recording, analysis, classification, prioritisation, taking corrective actions and limiting the effects of incidents”\(^\text{19}\).

Incident response teams operate in local government areas of responsibility and in individual companies; however, at the national level three teams are distinguished. Their English name is Computer Security Incident Response Team (CSIRT), and includes: CSIRT NASK, CSIRT GOV and CSIRT MON.

The first of them operates in the structure of NASK, the Scientific and Academic Computer Network – a national research institute. It is responsible, inter alia, for the coordination of incidents reported by local government, universities and individual citizens. The second one is run by the

\(^{15}\) Act of 26 April 2007 on Crisis Management [Dz.U., 2007, No. 89, item 590, Article 3(2)].

\(^{16}\) Act of 5 July 2018 on state cybersecurity system (Dz.U., 2018, item 1560).

\(^{17}\) Regulation of the Council of Ministers of 11 September 2018 on the list of essential services (...) for the delivery of essential services (Dz.U., 2018, item 1806).

\(^{18}\) Act of 5 July 2018 on state cybersecurity system [Dz.U., 2018, item 1560, Article 2(5)].

\(^{19}\) Ibid., Article 2(10).
Internal Security Agency and is supervised by the ministry responsible for digital affairs. It is responsible for the coordination of incidents reported by the main public authorities. The third team is run by the Ministry of National Defence for direct subordinates to the Minister of National Defence.

For example, the task of the Computer Security Incident Response Team – CSIRT GOV is: “[...] identifying, preventing and detecting security threats crucial from the point of view of the sustainment of the functioning of the state, public administration ICT systems or the ICT system networks enlisted as facilities, installations, devices and services of the critical infrastructure, as well as ICT systems of the owners and holders of facilities, installations or devices of the critical infrastructure referred to in Article 5b(7)(1) of the Act of April 26, 2007 on crisis management” 20.

Internet Resources

The Internet is divided into parts: the public one and the closed one. The first, open part is analogous to a passage in a shopping centre, where the owners of the sites display to the public the goods as advertisements. The second, closed part includes databases, technicalities, semi-finished products, drafts, etc. The ratio of these parts is probably 1 to 10 (The Internet resources are very difficult to estimate21). What we observe is only a small part of what we cannot see because it is a secret of the owners of particular websites. A special part of the Internet concerns resources to which the access route is purposely and automatically anonymous. This part of the Internet is called variously, e.g. dark web, tor or The Onion Router (i.e. a type of device connecting different computer networks). Contrary to the general opinion, accessing this area of the Internet is not difficult, and the protection in the form of onion (layered) routing gives an illusory feeling of impunity. Nevertheless, whether it is on the Internet or in real life, concealing criminal activity meets with reaction of the police and secret services. There is no such a notion as the illegal Internet; however, some online content is indeed illegal. The above applies to drug and weapons trafficking, dissemination of pornographic content involving children, and incitement to terrorist actions.

There are institutions obliged to fight hostile and criminal activities in cyberspace such as: the police and all civil and military defence agencies – the Internal Security Agency and the Military Counterintelligence Service. It is worth mentioning about the Police Cybercrime Bureau, which is supposed to create conditions for the “effective detection of perpetrators of crimes committed with the use of modern ICT technologies”22. It

should also be mentioned that there are plans to establish a new type of armed forces in Poland, the Cyberspace Defence Forces. For the time being, these are only project activities of scientists’ teams. For example, the Academic Center for Cybersecurity Policy operating as part of War Studies Academy in Warsaw, indicates that: “In the case of an extraordinary threat to the constitutional system of the state, security of citizens or public order caused by activities in cyberspace, which cannot be fought with ordinary constitutional measures – during a state of emergency – the Cyberspace Defence Forces could be ‘engaged’”\(^{23}\). According to authors from the Academic Centre for Cybersecurity Policy, the Cyberspace Defence Forces should be established as another, sixth type of armed forces, besides: land, air, special forces, navy and territorial defence forces\(^{24}\).

**Area 3. The Internet as a media environment**

Almost from the very beginning, *i.e.* from the early 1990s\(^{25}\), the Internet has been the environment for all types of media. The press, radio and television operate on the Internet. Nevertheless, some still also persistently maintain their specific forms of reaching audiences through newsprint, radio or television.

By the way, it is difficult to find a general definition of the media, and many authors present its different versions\(^ {26}\). Dieter Mersch, in his book entitled “Teorie Mediów”, describes the media sphere in a very ambiguous and enigmatic way: “It is neither individuality nor generality, form, matter, shape, content, figure, background – it occupies an undefined space, excluded from traditional divisions”\(^ {27}\).

The Internet has rapidly accelerated the process of defining what the media is: from an elite information provider, through a mass media, to a social network. It can be stated that in the Internet environment we are both receivers and senders of messages. Thanks to the media, we can stay active on the Internet both locally and globally. Anthony Giddens said this is our dialectic of the local and global ideas, so “a game of mutual interactions between local contexts and global tendencies”\(^ {28}\).

Manuel Castells calls the new Internet media reality: “mass self-communication, decisively increasing the autonomy of communicating subjects vis-à-vis communication corporations, as the users become both


\(^{24}\) Ibid., p. 36.


\(^{27}\) Mersch M, Teorie mediów. Wydawnictwo Sic!: Warsaw, 2010, p. 27.

senders and receivers of messages”29. The Internet media has also contributed to the state that nowadays we believe media descriptions more than our own senses. We can challenge any scientific authority, because the Internet will immediately provide us with arguments for or against particular statements. This indicates a productive backdoor for manipulation.

Fake news is false information disseminated in the media, especially Internet ones, usually used for disinformation or defamation. Fighting this type of fake news is difficult because, as the old saying goes, a lie told often enough becomes the truth. Nevertheless, there are many initiatives aimed at unveiling fake news. Here are a few that track disinformation in the Polish media space:

— FakeNews.pl portal (https://fakenews.pl/), run by the We Counter-Disinformation Foundation30;
— Demagog Association portal (https://demagog.org.pl/)31;
— Stop Disinformation portal (https://panoptykon.org/stop-dezinformacji-powiedzien), run by the Panoptykon Foundation32;
— I check project (https://sprawdzam.afp.com/list), run by the French agency AFP (operating since April 2019, as one of the first projects of this type in Poland)33;
— Konkret24 portal (https://konkret24.tvn24.pl/), run by TVN34;
— FakeHunter portal (https://fakehunter.pap.pl/), launched by the Polish Press Agency35.

Attempts to describe and expose entire strategies of faking reality, defamation campaigns, or creating so-called media bubbles are made to a lesser extent. There is also a lack of reflection on the information security of the state. Joanna Taczkowska-Olszewska notices that: “Information security is not a legal concept, which means that in the Polish legal system there are no common legal regulations in which the legislator decided to use this notion. Thus, it is impossible to find a legal definition of this concept. At the same time, it is easy to learn that this term has gained autonomy both in the field of security science, and has become a carrier of concepts and solutions of a regulatory nature”36.

31  Portal Stowarzyszenia Demagog.
36  Taczkowska-Olszewska J, Bezpieczeństwo informacyjne jako kategoria prawna. Ujęcie teoretyczne, [in:] Kitler W, Taczkowska-Olszewska J (Eds), Bez-
The creation of social media has given the impression that each of us can be equally an editor and a publisher. Nothing could be more wrong. The media world is still (maybe even more than before?) dependent on big players, corporations with great funds and specialised tools. The largest currently dominant companies in cyberspace are: Google, Amazon, Facebook, Apple and Microsoft.

Some Facebook users may have already come across so-called Community Standards\textsuperscript{37}. Not complying with these standards may result in restrictions from the owner of this social network. Restrictions are usually preceded by a message such as: “The publication of your content may be impossible due to continuous violation of our Community Standards. We’ve already limited the distribution of your site and we introduced restrictions on it.” The actions of large Internet companies that monopolise the markets, including social media, raise concerns of individual countries. For example, in December 2020, the US government filed a lawsuit in which “Facebook was charged with anti-competitive actions and the use of market dominance to collect consumers’ data”\textsuperscript{38}.

The process of defining threats related to information security in the era of globalisation is also beginning in Poland. Patrycja Szostok states: “The information security doctrine, to be complete, should also pay attention, which is extremely rare, to the media security of the state. […] Media security also concerns a relative independence from external sources of information, which requires the maintenance of domestic news agencies, and legislation, which regulates the participation of foreign entities in the media markets or limits the possibility of concentration of funds. These are issues that are regulated in separate legal acts, but are rarely considered as an element of information security of states, which seems to be an unacceptable oversight in the era of media globalisation and the threats it poses”\textsuperscript{39}.

\textbf{Area 4. The Internet as a new social environment}

For a long time, the Internet has been analysed as a new social environment and thus as a subject and area of social psychology research. Jan Zająć and Krzysztof Krejtz write: “The phenomenon of the Internet derives from the fact that from a social point of view it is now much more than just a communication technology. For many social groups, it has become

\textsuperscript{37} Stanowisko społeczności.


a natural social environment, allowing for the satisfaction of most social needs and motivations. It is employed not only to search for information, but also to make and maintain friends and close relationships. What is more, the network is also an area of forming new communities and social and cultural norms.

The point is that we are witnessing new phenomena being the result of relations made in the network, and so far we are not able to describe and define them properly. Anthony Giddens characterised the current era in the following way: “The modern era is mostly distinguished from all the preceding periods by an extraordinary dynamism. The modern world “escapes”: not only is the pace of changes incomparably faster than in any previous system, but also unprecedented is their scope and radical influence on existing practices and social behaviour.”

Jean Baudrillard, the creator of the simulacrum theory, points at the deep overlapping of the real and imaginary world. We domesticated the unknown world by giving it a description, some characteristics or signature. However, there are so many of these artificial signs that we no longer understand them and associate them with their original meaning. That is why, with time they start to live their own lives. “Abstraction today is no longer a map, a double, a mirror or a concept. The simulation does not apply for a territory, a being or substance. Instead it is generating, by using models, unreal and rootless reality – hyperreality.” Thanks to this theory, it is easier to understand what the virtual world stands for in the Internet era. The imagined net-world imitates real existence and causes duality or division of their reality as a consequence. Unfortunately, this can be compared to the situation of a sick person who simulates the disease so well that they actually finally fall ill.

Virtual reality influences the behaviour of particular people and social groups. It is a field to provide analysis and research, also in the context of the security of individuals and societies. Yet, another phenomenon that needs attention in this respect is artificial intelligence and self-learning machines. The view of machines taking over the world is still science fiction. Nevertheless, it often happens that we exchange thoughts and feelings on some discussion forum; however, we do not talk to another human being, but only to a machine that faithfully pretends to be a person. This is already a new reality. This artificial being on the Internet is called a bot, which automatically tries to imitate human behaviour. When someone uses bots for manipulation, we as recipients are struggling with ordinary embarrassment, or ... with a dangerous situation in the area of cybersecurity.

Conclusions

In the context of cybersecurity, the four presented areas – the law, defense system, the media on the Internet and new virtual reality – have to be analysed together. Security in cyberspace can be created only if all of these areas are consistently taken into account.

Adopting an effective cybersecurity strategy depends on defining what cyberspace actually means. The task is difficult as we are considering a constantly changing area that we are trying to identify. We are witnessing that cyberspace is expanding and cumulating at the same time. We are transferring more and more of our public, business and private activities to the virtual sphere. Therefore, we have to take into account that cyber-reality will constantly bring new types of law violation. Security in cyberspace will be ensured by building a comprehensive system secured by appropriate state and private institutions. These must take care of critical infrastructure, digital services and the secure information loop, as well as develop ways to respond to any incidents related to computer security.

The Internet is the environment for all media, which is why cyberspace security is as important as the protection of our information.

Presently, the Internet has become a new social environment. For many users, the Internet network replaces the existing interpersonal relationships. No one knows to what extent and why the web has gained such great influence on us. An even greater question may be the development of artificial intelligence and its evolution on the basis of the Internet. This is why the above also needs to be taken into consideration when creating an overall cybersecurity system.

References

Publications

Ekspertyza w zakresie obowiązujących aktów normatywnych regulujących środowisko prawne działania nowotworzonych Wojsk Obrony Cyber-
Four areas of cybersecurity – discussion of the subject area


Legal Acts


Act of 5 July 2018 on state cybersecurity system (Dz.U., 2018, item 1560).

Rozporządzenie Rady Ministrów z 11 września 2018 w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych (Dz.U., 2018, item 1806).

Other sources


**Keywords:** cybersecurity, cyberspace, cyberspace law, Internet, media, artificial intelligence

**Summary:** The article briefly discusses four areas that should be considered when analysing the concept of cybersecurity: the legal aspect of cyberspace, the state security system, the specificity of the media in the Internet environment, and last but not least – new virtual reality emerging in cyberspace. In the context of cybersecurity, all of these research areas have to be considered together.