Przegląd Europejski, ISSN: 1641-2478
vol. 2021, no. 3
doi: https://doi.org/10.31338/1641-2478pe.3.21.5

(In)security of the functioning of the information society in the cyberspace

Waldemar Krztoń, *Ignacy Łukasiewicz Rzeszów University of Technology (Rzeszów, Poland)*
E-mail: wkrzton@prz.edu.pl
ORCID ID: 0000-0001-8292-4327

Abstract
The aim of the article is to identificate and analyse the most important risks associated with human functioning in the network as a member of the information society. The main research problem is the question of what dangers threaten a human functioning in cyberspace? An analysis of the material gathered through its examination, clarification and categorisation enables to solve the research problem. This provides the basis for formulating the thesis that the functioning of the information society in cyberspace includes many positive qualities, nevertheless, one should not forget about the dangers in the form of inundation of information, mental dependence, or criminal activity. The most important, however, is conscious and reasonable exertion of the Internet by users.
Keywords: security, cyberspace, cybersociety, cyber-risks, information society, Internet

(Nie)bezpieczeństwo funkcjonowania społeczeństwa informacyjnego w cyberprzestrzeni

Streszczenie
Celem artykułu jest przeprowadzenie analizy dotyczącej identyfikacji najważniejszych zagrożeń związanych z funkcjonowaniem człowieka w sieci jako członka społeczeństwa informacyjnego. Głównym problemem badawczym jest zatem pytanie, jakie niebezpieczeństwa zagrażają człowiekowi funkcjonującemu w cyberprzestrzeni? Rozwiązanie problemu badawczego umożliwiła analiza zgromadzonego materiału poprzez jego zbadanie, objaśnienie i kategoryzację. Stanowiło to podstawę do sformułowania tezy, że funkcjonowanie społeczeństwa informacyjnego w cyberprzestrzeni zawiera dużo pozytywnych cech, niemniej nie należy zapominać o zagrożeniach w postaci: zalewu informacji, uzależnienia psychicznego, działalności przestępczej. Najważniejszym jest jednak świadome i rozsądne korzystanie z Internetu przez użytkowników.
Słowa kluczowe: bezpieczeństwo, cyberprzestrzeń, cyberspołeczeństwo, cyberzagrożenia, społeczeństwo informacyjne, Internet

At the turn of the 21st century, many changes occurred in the functioning of the economy and the state in the life of society and the individual, caused by the unexpectedly rapid development of ICT (information and communication technologies). The turning point was the emergence and snowballing development of the Internet, which enabled the exchange of information on a global scale and facilitated communication. The Internet is now an essential part of functioning in all areas of social, economic, political, and cultural life. ICT covers most of public and private operations. It is a means of gaining knowledge as well as a source of information. The Internet as a tool, through which network computers interact (communicate), has enabled functioning in cyberspace, i.e. virtual space. Consequently, state borders and the public and private divide do not constitute significant obstacles. These fundamental changes give rise to new opportunities, challenges, risks, and security threats.

Therefore, ensuring security in the net is a major challenge for the state. The premises that caused the formation of the information society continue to actively influence its development. Living in an information society means, inter alia, easier access to information, while the use of network structures promotes social activity. The functioning of the information society in cyberspace contains a lot of positive features: the speed of information circulation and the easiness of finding it, the convenience of using email, the possibility of creating new forms of social life. Nevertheless, one should not forget about the dangers.

Hypothesis and research metods

Undertaking the research let sketch some problems concerning the functioning of information society in a new area, virtual space. The aim of the research is to identify the dangers of human functioning in cyberspace as a member of the information society. The accomplishment of the research aim required to define the research problem: what are the dangers to the human functioning in cyberspace? Referring to the research question, the author formulated a research hypothesis that functioning of the information society in cyberspace has a lot of positive features, nevertheless, it has the dangers in the form of flooding of information, mental addiction, or criminal activity. The research methods used in this research are: analysis, synthesis, and comparison. The used methods let verify the determined hypothesis and accomplish the formulated research aim.

The rise of the information society

The information society is already functioning (Wegner 2020). It is written and discussed a lot by investigating its aspects and components. Various manifestations of the action of the information society are noted. It is characterised by the undoubted possibility of a quick and cheap circulation of information. There is also a gush of information that is unnecessary or even simply harmful, which is problematic by inability to be verified and defended against. Information is manipulated, even disinformation activities are carried out with its use more and more frequently (Oleksiewicz, Krztoń 2017: p. 75).

In most definitions (Golka 2008: p. 80–81), the term "information society" is understood as one, whose essential component remains information, which is produced, processed, collected, communicated, and received. This is a necessary factor in its functioning. The Internet, the computer and all devices, tools or digital technologies are the most important areas of life and work for its members. Information as a product, a commodity, a raw material has become the essence of modern civilisation and its lifeblood.

Pervasive competition promotes the search and sale of information, particularly the one, which is new, relevant, and attractive. This leads to economic, political, social and cultural changes, the spread of which has gained an unprecedented rate so far. According to Manuel Castells "New information technologies, changing the nature of information processing, affect all spheres of human activity" (Castells 2007: p. 86).

The term "information society" was introduced by Tadeo Umesao in 1963 for the first time. This concept is an attempt to generalize the display of key constituents, mechanisms of functioning, and the hallmarks of a new phenomenon. Naturally, in the literature of the subject, many proposals for naming this phenomenon can be found, among others, "knowledge society" (Drucker 2002: p. 446), "network society" (Castells 2007), "third wave" (Toffler 2001).

The information society is a new kind of society. It is a society:

1) in which the production of information and intangible assets becomes the driving force for formation and development (Juszczyk 2000: p. 12);
2) in which all persons are allowed free access to create, receive, share and use information and knowledge, which contributes to their social, economic, cultural and political development (Wrycza 2010: p. 471);
3) which has a rich means of communication and information processing underpinning the majority of national income and providing the livelihood of most people (Pinter 2008: p. 23);
4) in which information technology and telecommunications have an ever-increasing role in all areas of social life, and in which these technologies have changed the foundations of social structures and processes and caused huge changes in politics, economy, culture and daily life (Karvalics 2008: p. 34).

One should agree that the information society is shaped through widespread access to computers and the Internet and knowledge of their use. The computer and smartphone are the devices and technology most characteristic of the present time. However, this rise and development of the Internet most likely was the cause of the formation of the information society and the Internet became an inherent part of it.

People have long communicated using different networks, but only recently as a result of the use of the Internet, which is a means of communicating many with the many, and at one time and on a global scale, have become a new value. Networks created by the Internet are numerous integrated nodes, however, largely independent of each other, between which information flows. Besides, they function as open structures, capable of continuously developing and thus, connecting new nodes (Golka 2008: p. 82–83).

Personal computers (PCs) and smartphones became the most distinguishing components characterising the information society. In modern times, they are a versatile

and common means of contacting, connecting with other devices. The Internet is co-created by all members of the community who use it and also those who function in the space of its operation.

Information society influences different areas of the functioning of the person: technological, social, economic, and cultural (Wrycza 2010: p. 471):

1) technological — development of new technologies, high degree of use of modern technologies and the Internet by society;
2) social — development of means of communication, access to electronic products and services, creation of online communities;
3) economic — professional development through new technologies, the impact of society on economic activity;
4) cultural — a high level of information culture, virtual reality, electronic entertainment.

The 21st century society has mostly been shaped through innovative ways of information circulation. The contemporary process of transmitting information in a globalised world enables it to be relatively integrated.

The information society, and primarily the Internet, contains a lot of positive features: the transfer of many spheres of mass culture based on radio and television to the network; the convenience of email, the speed of information circulation and the ease of finding it, the ability to create new forms of social life. Nevertheless, new problems arise in other areas: progressive alienation in work and daily functioning, inundation of information, exacerbation of differences between rich and poor countries, mental dependence, and mainly functional dependence on information systems (Golka 2008: p.90).

Nor should we forget about the dangers of the information society in the form of criminal acts (Jaroszewska 2017): theft of information, intellectual property and money, destruction of programmes and files, pedophilia and pornography, dissemination of dangerous beliefs and ideologies, communication of criminal and terrorist organisations, arms and drug trafficking, fraud and extortion, etc.

Tomasz Goban-Klas and Piotr Sienkiewicz assume that further development of the information society can proceed according to the following variants (Goban-Klas, Sienkiewicz 1999: p. 51):

1) firstly, it can develop in economically and technologically advanced countries, contributing to their further development in all aspects of life;
2) secondly, there may be a recourse of social and individual development precisely as a result of the dominance of information technology;
3) thirdly, sustainability may take place with the assumption that the beneficial effects of information technology will be exploited while remembering (and taking into account) the negative ones;
4) fourthly, it is difficult to prejudge what further development will be, since the effects of using technology depend on people to a small extent.

Current knowledge of the functioning of the information society is insufficient, there are many uncertainties and gaps. A large part of what we think and write about the information society in a short time may become out of date. We are certainly unable to predict

the further shape of the development of the information society. Nevertheless, it can be noted with great certainty that this society will have to continue and develop, because there is no longer a retreat from it.

This is confirmed by Manuel Castells who writes, "for as long as you wish to live in a society, here and now, you will have to deal with a network society. For we live in the Internet Galaxy" (Castells 2003: p. 313).

Cyberspace as an area for communicating the information society

It is worth directing attention to the classical, fixed and essential understanding of the term *space* (Sienkiewicz 2013: p.104):

1) first — initiated by Democritus and the Stoics and then developed by Newton, the space was identified with a kind of place, the vacuum in which individual entities were to be filled;
2) second — the understanding of this concept giving it an absolute dimension is Immanuel Kant's idea of spatiality as a form of conceptual recognition of the reality being a subject of experience;
3) third — an expression, formulated by Gottfried Wilhelm Leibniz and restored by Albert Einstein, that linked space to material existence, that is, reality.

Many attempts to interpret or reinterpret the concept referred to as cyberspace can be found in the literature. Piotr Sienkiewicz lists its basic grasps (Sienkiewicz 2013: p. 108):

1) cyberspace is simply the Internet, its resources and services as well as users;
2) cyberspace equates to virtual reality generated by the computer, network, and Internet;
3) cyberspace constitutes, in essence, a social mega-network — a "network of networks", whose individual and group participants (communities) exploit global resources provided by the Internet (general — network);
4) cyberspace is simply an evolving dynamic complex system, and it should be viewed first, whether its technical, informative, or social aspects are displayed.

Cyberspace is used to process, store and transmit information, and the essence of cyberspace is to use information in a digital form. In a narrower sense, cyberspace is regarded as the Internet and the World Wide Web, which connect computers and provide information exchange between people. Therefore, the Internet provides and facilitates a global communication space for political, economic, social, and cultural activities. Cyberspace creates a digital social space, and social media, news portals, discussion forums, databases, etc. are used for this. In a broader sense, cyberspace is a social information space, but also an infrastructure: specialist equipment, telecommunications devices, Internet services, multimedia, and hypertext systems.

This is supported by Dominika Dziwisz, who states that: "...cyberspace contains the Internet and any other computer networks, for example, private networks that are separated from the Internet. It is a hybrid of telecommunications lines, television, and computers that converge with each other" (Dziwisz 2015: p. 37).

One of the manifestations of the existence of "cyberspace" and at the same time, its feature is virtuality (Unold 2015: p. 173). Virtuality blurs the difference between a *real* sphere and *virtualis*, truth and pretence, copy and original. Virtuality should be regarded as a potential feature of cyberspace and networking as a constitutive one, whereas given the communication qualities, interactivity, multimediality, and hypertexticity cannot be omitted. A feature of virtuality is the multi-sense experience of transmission and a balanced level of simulation owing to the technical capabilities of creating illusions. Since the beginning of the technical possibility of virtual reality realisation, features such as simulation, interactivity, telepresence and, above all, "immersion" in the artificially plotted world of events and fiction have been exhibited.

Virtual reality connotes intrinsically with a computer equipped with special device, which delivers deep immersion and comfortable interaction. This device completed with adequate computer programme provides virtual impressions to the simulation participant. The most popular devices are google of virtual reality, also called cybernetic helmets until recently. It contributed to the fact that many people perceive virtual reality through the prism of these devices. In some way, they become the synonym for virtual reality (Lebiedź et al. 2018: p. 117).

Some experts of the topic propose to comprehend cyberspace with a human element and therefore propose the following term: "cyberspace is a time-dependent set of interconnected information systems and human users who cooperate with these systems" (Ottis, Lorents 2010). This important complement to the understanding of cyberspace shows that the operation of this space is possible thanks to users, that is, people.

Therefore, we can talk about the emergence of a new "cyberenvironment" of a human, which is already becoming a digital complement to the existing environment of man, and sometimes becomes its alternative. The concept of cybersociety emerges frequently in literature next to the term cyberspace. Considerations on the characterisation of cyber society are continuing and there does not seem to be any agreement reached in any time soon, even more so as it is an interdisciplinary problem. Nevertheless, Agnieszka Lekka-Kowalik lists three features of cybersociety (Lekka-Kowalik 2003: p. 18–19):

1) in cybersociety most activities, whether individual or social, take place *on-line*. *On-line* activities are believed to be in some substantial respects better than analogous actions performed *off-line*. Therefore, it is proposed to move more and more activities into cyberspace. It is also believed that this transfer has, or will have, socially positive consequences in the near future: e.g., competition between companies will increase thanks to an increase in the ability to choose the individual, the never-beleaguered regions will have a better chance of development, people will be able to develop their interests, etc. having saved time, energy and money in the course of performing vital activities. Cybersociety is therefore seen as an environment better for human development and self-realisation;
2) cyber society is an information technology society not only because telecommunications and information technology techniques are used in the activities, but also because these techniques are seen as a significant production

factor and the use of ICT as a versatile development factor. The workforce is also mostly composed of domestic product is created within the broadly understood IT sector;

3) cyber society is also an information society because information is the primary production factor, the main commodity, and determinant of action. It is assumed that the quantity and speed of collection, processing and transmission of information has social positive consequences. By increasing citizens' access to information, the formation of channels of horizontal social communication, and the ease of organising groups of information sharing and pressure social, the actual participation of citizens in the governance of the country will increase. The geographical and financial barrier to human contacts will disappear, which will promote global solidarity and understanding.

People living in an information society need to communicate with others and exchange information. They share information among themselves through social media. The development and spread of social media have decisively changed the way people, communities, and organisations communicate. Social media operates on the basis of Web 2.0 technologies and allows users to create and exchange information content (Ślązak 2019).

The popularity of participating in the functioning of social media and its use results from several sources (Ngai et al. 2015: p. 33):

1) human behaviour at the individual level:
- attributes of personality — openness, conscientiousness, extraversion, settlement and neuroticism can develop the behavioural intentions of social media users,
- acceptance of technology — observed ease of use and perception of the utility of new technologies in relation to people's attitudes towards their adoption;

2) social behaviours — social factors such as:
- social impact, which includes social identity,
- social capital, which includes social interactions and social ties;

3) mass communication and its effect on people's behaviours.

The following social networking sites are most often distinguished (Karciarz, Dutko 2010: p. 16–17):

1) social — allowing you to establish and maintain virtual acquaintances such as Facebook.com, NaszaKlasa.pl, MySpace.com, Grono.net;
2) networking — the purpose of which is to create business networking, as well as to allow the application to thematic (industry) groups;
3) content — allowing users to share specific content such as videos, photos or music;
4) citizen journalism services — information sites having their origin in the work of social amateur journalists sending coverage and photographic material and video directly from the event venue, e.g. Wikinews.pl, iThink.pl, News24.pl, Interia360.pl;
5) discussion forums — virtual places of exchange of opinions centred around particular topics, e.g. Forum.Gazeta.pl, Forumowisko.pl;

6) blogs — sites presenting subjective opinions of people conducting them, mostly covered in chronological form of published posts;
7) repositories — ordered collections of documents such as dictionaries, encyclopedias, databases, etc.

Today, the presence on social media is not only communication between people, but also the possibility of professional development or the production of financial benefits. In principle, all counting domestic and international companies operate on social media conduct marketing, advertise new products, and most importantly, seek active customer commitment.

Perception of cyberspace merely through the lens of the Internet seems like a big simplification, as does attribute coherence and homogeneity to the Internet. Functioning in cyberspace creates the need of changes and updates necessary for the proper fulfillment of specific functions by the state and society. These are the effects of civilisational development in scientific, technical, and technological areas. As a result of these changes, many new modernised areas of economic, social, formal-legal activity, the creation of rational social behaviour rules, and security programmes have been created in cyberspace (Wegner 2020).

Network activities can be grouped into areas, for example:

1) economic activities — e-business;
2) buying and selling activities — e-trade;
3) educational activities — e-education, e-science;
4) public activities — e-government;
5) the activities of social relations — e-communities;
6) communication activities — e-mail.

Cyberspace is a space of increased risk and new threats. The more knowledge of this phenomenon, the more uncertainty grows. The increasingly extensive structures of the "virtual" community are conducive to producing many side effects in the form of theft, intrusions, spams and viruses (Krztoń 2017: p.209).

Threats arising from functioning in cyberspace

At the same time, new risks and threats arising from the specific nature of the network are emerging with the development of the information society. The snowballing amount of information available causes the lack of ability to process and perception by human, which impedes his normal functioning. Information, when spreading very quickly, makes it difficult to verify and respond adequately to it. The most significant challenges and risks can include psychosocial, privacy, and criminal activities (Lizut 2014).

The transformation of cyberspace through the development of ICT has resulted in a shift in the relationship between people from personal to digital on the web. Some people are starting to be exhausted, while, others have become addicted to the Internet and contacts in cyberspace. Research demonstrates three dimensions of ICT overload

by users: communication overload 86%, information overload 55%, system functions overload 47% (Wojciechowska-Filipek, Ciekanowski 2016: p. 37).

Increasingly, the problem of network and technology overload of workers performing their duties, as well as people in ordinary activities, begins to occur and grow. Society is increasingly reliant on digital technology and information far more than ever before. Users feel fatigued with incessant communication on the network, they are connected to it virtually 24 hours a day, 7 hours a week. They have to receive emails, texts, and phone calls at work all the time, on the way home they do not part with phones and tablets, and at home they immediately connect to the network to appear on social media (Wojciechowska-Filipek, Ciekanowski 2016: p.38). After a time of fascination with the new form of connectivity, people begin to feel exhausted by the obligation of incessant communication, and also report more and more doubts about the value, legitimacy and quality of content distributed on the web.

At this time cyberspace users are bombarded with information, virtually all of them can develop and post information on the Internet. As a result, the quantity and size of information increase at a rapid rate, which leads to the fact that obtaining valuable and timely information is a difficult task. Choosing necessary, specific, up-to-date and true information among contradictory, inconsistent and inadequate can be a challenge and may cause a sense of uncertainty, risk, anxiety, and danger.

Excess information often exceeds the capacity of the human mind to process and perceive it, leading to information overload that causes the inability to understand the subject in question, hindering the right decision-making and actions appropriate to the situation. This phenomenon occurs when potentially useful information received becomes an obstacle rather than an aid (Jackson, Farzaneh 2012: p. 523-532). It must also be noted that each person has different abilities to search, analyze and interpret information, especially in the case of uncertain and complex information.

In the literature of the subject, we can find information that, despite many benefits of functioning in cyberspace, there are also negative psychosocial effects for some users, and this can lead to pathological and/or problematic use of the Internet or even Internet addiction. These phenomena are regarded as an important mental health problem and can affect people of all ages, hurt a particular person as well as his family. Several major Internet addictions can be distinguished (Gogołek 2006: p. 319):

1) computer addiction — in this case, the user does not have to be in cyberspace at all, it is enough that he spends time in front of the computer. It is not important what he does with it. An addicted person not only treats the medium anthropomorphically, but even as a part of himself (his brain, memory);
2) addiction to virtual games — involves addiction to virtual games as well as obsessive gambling. Underage users are provided with information related to violence and aggression, thus forbidden by parents and thus desired. For adults, games become an alternative to the real world. Whereas, e-gambling can result in serious financial and legal problems;
3) information overload — compulsory web browsing, including databases. It occurs with a surplus of information — chaotic flipping of information found on

the web, participating in multiple discussion forums, and conducting multiple conversations simultaneously;

4) Internet socio-mania — this is an addiction to online social contacts. The user makes new contacts only and exclusively through the network, usually to the detriment of normal social relationships. Such a situation, as a rule, is accompanied by emotional withdrawal, mental absence, apathy, extinguishing feelings;
5) Internet erotomania — mainly involves watching videos and photos of pornographic material or conversations on sex-themed chats. This phenomenon is dangerous, when a material with pornographic content is hit by people with disorders in the emotional sphere or minors.

The privacy sphere of human functioning is protected, and the right to privacy is treated as a fundamental right of the individual. In the age of information, the right to privacy takes special meaning, and it is understood as the right of the individual to decide: when, how, and to what extent the resource of information relating to it can be shared with others (Braciak 2002: p. 296). This right is also covered by the right to privacy of information and includes personal data control during collection, analysis, testing, duplication, and distribution in ICT systems.

When conducting a transaction in cyberspace, users leave a large number of information and data necessary to complete the transaction, e.g. (Wojciechowska-Filipek, Ciekanowski 2016: p. 45):

1) name, and email, with every contact with the supplier of products and services;
2) name, address and telephone number, with each purchase of a product supplied by a courier company;
3) the card number, the holder's details, and the expiry date, with each payment on the network by card;
4) often when purchasing a product or service, you need to provide additional information, for example: shopping preferences, frequency, occupation, age, etc.

Modern ICT provides powerful opportunities for collecting and processing personal information and building a pattern of behaviour, preferences, as well as identification of individuals. These resources can be used variously, among other things, for trading personal data. Most frequently, it is not known who collects data, to whom they are transferred, in what form, and under what circumstances. Data collection is carried out in a hidden manner, mostly without the knowledge and full consent of network users.

Privacy threats may apply to (Lee, Kwon 2010: p. 5193):

1) excessive collection of information;
2) secondary use of information;
3) intentional or accidental errors in personal data;
4) unauthorised access to information.

Functioning in cyberspace can also lead to threats arising from criminal activities. Such activities in cyberspace are financially and materially motivated. According to Jerzy Kosiński and Sebastian Kmiotek, the term cybercrime, or criminal activities in cyberspace, refer to four types of crimes (Kosiński, Kmiotek 2010):

1) traditional forms of crime, such as fraud or forgery, which, in the context of cybercrime, relate to crimes committed using electronic IT networks and information systems;
2) publication of illegal content in electronic media (e.g. material related to sexual exploitation of children or calling for racial hatred);
3) crimes typical of electronic communication networks, such as attacks against information systems (DoS attacks, intrusions into computer systems, pharming, violation of the integrity of information systems);
4) digital multiplication and dissemination of works or artistic performances without the consent of the authorised person in order to obtain a benefit.

An example of social engineering used by cybercriminals might be "BLIK extortions" by means of social network. In the middle of 2019, there were numerous illegal activities, which used the mobile payment system "BLIK". They were distinguished by a scenario based on kidnapping information. The practice consisted of two stages. In the first one, the attacker was distributing the information about child's kidnapping in a shopping centre. Links in posts referred to the websites posing as news platforms, where the kidnapping was described. The whole incident was registered by monitoring system, and the fake news websites asked for help in finding the child. At the moment of clicking in the video the victim was informed that due to drastic content, the material is available only for users who are more than 18 years old. In order to verify the age, the user had to sign in via Facebook. After choosing "sign in" option, the victim has been shown a fake login panel located under the same domain as the information service. Providing login and password, so as not to arouse any suspicions, the victim was redirected to the official website of Centre for Missing People – zaginieni.pl. To sum up, in the first stage the attacker gained login data to facebook.com from the unaware victim. To achieve that, the attacker distributed massive spams, which informed about the kidnapping focusing on a particular child, city, or shopping centre. After stealing logins and passwords, the attacker was able to pose as the victim. Sending information about the kidnapping via victim's profile on Facebook occurred to be very effective. The sensational post content provoked many people to share it what built greater reach for the fake login panel. At this moment the attacker moved to the next stage. After signing into the victim's account, the cybercriminal contacted friends from the list. The violator described them different stories e.g. about car's breakdown while a long trip, the necessity to transport it by car carrier trailer, and lack of cash or credit card. In relation to this, the attacker asked a friend to issue a check or BLIK code, which would allow the violator to withdraw cash from the nearest ATM. Of course, everything was supposed to be a short-term loan, which would be repaid right after arrival. Despite quite complicated scenario, this method was the most effective. The victim usually did not think that the attacker is communicating via friend's account. Additionally, in most cases it was already too late, when the fraud was detected, and which impeded targeting the violator (CERT Polska 2019: p. 46).

Among common methods and techniques of criminal activities, experts include (Białoskórski 2011: p. 68–69):

1) mind games — cybercriminals have increasingly resorted to psychological warfare. "Daily" scenarios are being used more and more frequently in place of earlier unlikely offers of sudden receipt of a large amount of cash. E.g. "spear phishing" is increasingly being used, pretending correspondence from friends and acquaintances, in which users are induced to provide account names and passwords. Such type of personalised tricks is directed at consumers.
2) social engineering — cybercriminals attack large groups of victims associated with networks and social networking sites. The developers of malware make a profit on their popularity by creating fake profiles and pages containing adware, spyware, and trojans. Cybercriminals also collect information on members of online communities and use copies of their profiles for criminal purposes;
3) data leaks — data are still vulnerable to theft even without the need of sophisticated methods and cybercriminals very often use them. For example, the use of numerous passwords for both professional and personal activity makes passwords easy to guess very frequently. Unsecured removable memory facilitates information transfer, and technology convergence introduces an additional risk;
4) bot networks — networks of remote-controlled "zombie" computers are now the most widespread tool used by computer thieves, used for illegal spamming, spreading pornography, password and identity theft.

Conclusions

In the age of an informational society, information plays a fundamental role in all spheres of human activity. Changes in daily human functioning resulted in rapid development of ICT, particularly the Internet. A uniquely important role in this area is played by cyberspace as a means of dissemination of information, media integration, and social activity. Access to information, products, services, education, health and offices has become common without territorial or time restrictions. Users of cyberspace gained wide access to information resources, as well as an unlimited opportunity to produce and transmit information.

To sum up the considerations, on the basis of the studies carried out, it should be concluded that functioning in cyberspace brings not only advantages, but also some kind of opportunities, challenges, risks, and threats. There are the most frequent dangers in the form of flooding of information, mental addiction, or criminal activity. The main risks to the individual are psychosocial risks associated with computer, network and technology addictions, which is a fundamental health problem at the moment. In addition, people who operate on the network are exposed to risks associated with loss of privacy and personal information. Attacks aimed at databases can disorganise and destroy the lives of the information community in particular. Cyber-attacks are significant danger, which fundamentally affect different spheres of life negatively and threaten the interests of individuals. Criminal activities on the web result in measurable social, financial and material losses. Due to the complexity of security issues, it is difficult to find a full and

absolutely secure solution to operating safely on the network. The most important is the careful and prudent use of the Internet by users, which becomes a requirement of modern times. Therefore, the necessity for educational activities is important. Education should be conducted towards the dissemination of knowledge of the risks present and the formation of users' awareness of the possibility of minimising the risk associated with functioning in cyberspace. The substantial content of the paper allows to acquire knowledge of the most important dangers present in cyberspace connected with the information society. The security of operation in cyberspace requires that the users and gathered information resources are provided with adequate methods for the safe processing, storage, and transmission of them.

Waldemar Krztoń – Ph.D., university professor at the Department of Project Management and Security Policy at the Ignacy Łukasiewicz Rzeszów University of Technology. Scientific interests: problems of information security, warfare and armed conflicts from the historical, contemporary and prognostic point of view. Selected publications: *Struggle for Information in Cyberspace in the 21st Century* (2017); *Human Dignity as a vital value for an individual's security. Analysis of Selected Views* (2018).

Waldemar Krztoń – doktor, profesor uczelni w Zakładzie Zarządzania Projektami i Polityki Bezpieczeństwa na Politechnice Rzeszowskiej im. Ignacego Łukasiewicza. Głównym przedmiotem zainteresowań naukowych są problemy bezpieczeństwa informacyjnego oraz wojny i konflikty zbrojne w ujęciu historycznym, współczesnym i prognostycznym. Wybrane publikacje: *Walka o informację w cyberprzestrzeni w XXI wieku* (2017); *Godność ludzka jako istotna wartość bezpieczeństwa jednostki. Analiza wybranych poglądów* (2018).

References:

BIAŁOSKÓRSKI Robert (2011), *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku. Zarys problematyki,* Warszawa.

BRACIAK Joanna (2002), *Prawo do prywatności*, in: Bogusław Banaszak, Artur Preisner (ed.), *Prawa i wolności obywatelskie w Konstytucji RP*, Warszawa.

CASTELLS Manuel (2003), *The Internet galaxy. Reflections on the Internet, business and society*, Poznań.

CASTELLS Manuel (2007), *Rise of the network society*, Warsaw.

CERT POLSKA (2019), *Krajobraz bezpieczeństwa polskiego internetu*, Raport roczny 2019 z działalności CERT Polska, https://www.cert.pl/uploads/docs/Raport_CP_2019.pdf (12.05.2021).

DRUCKER Peter Ferdinand (2002), *Myśli przewodnie Druckera*, Warszawa.

GOBAN-KLAS Tomasz, SIENKIEWICZ Piotr (1999), *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania*, Kraków.

GOGOŁEK Włodzimierz (2006), *Technologie informacyjne mediów*, Warszawa.

GOLKA Marian (2008), *Bariery w komunikowaniu i społeczeństwo (dez)informacyjne*, Warszawa.

DZIWISZ Dominika (2015), *Stany Zjednoczone a międzynarodowe bezpieczeństwo cybernetyczne*, Kraków.

JACKSON Thomas, FARZANEH Pourya (2012), *Theory-based model of factors affecting information overload*, "International Journal of Information Management", vol. 32, issue 6, p. 523-532. DOI: 10.1016/j.ijinfomgt.2012.04.006

JAROSZEWSKA Iga (2017), *Wybrane aspekty przestępczości w cyberprzestrzeni. Studium prawnokarne i kryminologiczne*, Olsztyn.

JUSZCZYK Stanisław (2000), *Człowiek w świecie elektronicznych mediów – szanse i zagrożenia*, Katowice.

KARCIARZ Magdalena, DUTKO Maciej (2010), *Informacja w Internecie*, Warszawa.

KARVALICS Laszlo (2008), *Information Society — what is it exactly?* in: Robert Pinter (ed.), *Information society. From theory to political practice*, Budapest.

KOSIŃSKI Jerzy, KMIOTEK Sebastian (2010), *Międzynarodowa współpraca w zwalczaniu przestępczości*, http://www.dobrauczelnia.pl/upload/File/KONFERENCJE/Cyberterroryzm/kosinskikmiotek.pdf (10.04.2010).

KRZTOŃ Waldemar (2017), *Walka o informację w cyberprzestrzeni w XXI wieku*, Warszawa.

LEE Yonnim, KWON Ohbyung (2010), *An index-based privacy preserving service trigger in context-aware computing environments*, "Expert Systems with Applications", vol. 37, issue 7. DOI: 10.1016/j.eswa.2009.12.072

LEBIEDŹ Jacek, KRZTOŃ Waldemar, STEFANIUK Barbara (2018), *Współczesne wyzwania bezpieczeństwa narodowego. Zarządzanie kryzysowe, wojna w cyberprzestrzeni, rzeczywistość wirtualna*, Warszawa.

LEKKA-KOWALIK Agnieszka (2003), *Czy cybernetyka wystarczy cyberspołeczeństwu?* in: Tadeusz Zastepa, Radowsław Chmura (ed.), *Internet i nowe technologie – ku społeczeństwu przyszłości*, Częstochowa.

LIZUT Joanna (ed.) (2014), *Zagrożenia cyberprzestrzeni*, Warszawa.

NGAI Eric, TAO Spencer, MOON Karen (2015), *Social media research: Theories, constructs, and conceptual frameworks*, "International Journal of Information Management", vol. 35, issue 1. DOI: 10.1016/j.ijinfomgt.2014.09.004

OLEKSIEWICZ Izabela, KRZTOŃ Waldemar (2017), *Bezpieczeństwo współczesnego społeczeństwa w cyberprzestrzeni*, Warszawa.

OTTIS Rain, LORENTS Peeter (2010), *Cyberspace: definition and implications*, in: *Proceedings of the 5th International Conference on Information Warfare and Security*, Dayton, OH, US, 8-9 April, p. 267-270, https://ccdcoe.org/library/publications/cyberspace-definition-and-implications (02.04.2020).

PINTER Robert (2008), *Towards getting to know information society*, in: Robert Pinter (ed.), *Information society. From theory to political practice*, Budapest.

SIENKIEWICZ Piotr (2013), *25 lectures*, Warsaw.

ŚLĄZAK Emil (2019), *Web 2.0 jako nowy wymiar Internetu*, https://viem.viennalife.pl/pl/artykuly/web-2-0 (19.02.2019).

TOFFLER Alvin (2001), *Trzecia fala*, Warszawa.

UNOLD Jacek (2015), *Zarządzanie informacją w cyberprzestrzeni*, Warszawa.

WEGNER Magdalena (ed.) (2020), *Społeczeństwo informacyjne w Polsce w 2020 r. Analizy statystyczne*, Warszawa.

WOJCIECHOWSKA-FILIPEK Sylwia, CIEKANOWSKI Zbigniew (2016), *Bezpieczeństwo funkcjonowania w cyberprzestrzeni – jednostki, organizacji, państwa*, Warszawa.

WRYCZA Stanisław (ed.) (2010), *Informatyka ekonomiczna.: podręcznik akademicki*, Warszawa.

Received: 29.12.2020. Accepted: 21.05.2021.