Agnieszka Dymicka*

Cybersecurity from the perspective of a new technology user

Abstract

New technologies are, in the world of advancing processes of globalization, scientific and technical revolution, one of the most important indicators for designing many areas of social life. The useage of information technology has initiated many social phenomena generating many previously unknown concepts, threats, and in response, new areas of expert and research interest. One of them is cyber security, which focuses on building national, European or international policies to secure the functioning of information systems.

The aim of this paper is to analyze and evaluate cyber security from the perspective of a user of new technologies. The applied research method will be a synthetic and analytical analysis of domestic and foreign literature in the field of new technologies and cyber security.

Key words: cyber security, cyber hygiene, new technology, information technology, digital technologies

* Agnieszka Dymicka, PhD Student, John Paul II Catholic University of Lublin, e-mail: adymicka@wp.pl.

New technologies. Conceptualizing the idea

New technologies and their impact on the economy being the basis of many studies and analyses contributed to the multiplicity of their definitions showing the perception of new technologies and their social impact from many perspectives.

Manuel Castells, in his book „Network Society" implemented the definition of new technologies after H. Brooks and D. Bell enriching it with new elements. Castells defines technology as: „the use of scientific knowledge to determine methods of doing things in reproducible ways"[1]. He classifies information technology as „a converging set of techniques in the fields of microelectronics, data processing (hardware and software), telecommunications, transmission, and optoelectronics"[2]. Unlike other researchers, Castells also includes genetic engineering in the field of information technology[3]. The Central Statistical Office's definition of information technology stating, that information technologies are: „technologies related to the collection, storage, processing, transmission, and presentation of information (i.e., text, images, and sound), including in particular computer (hardware and software) and communications"[4] is a definition that, compared to Castells' definition, does not include feedback and a clear indication of the role of knowledge in new technologies. The development of new technologies in the world does not proceed in an unambiguous way. New technologies are not a separate entity from the economy, culture, society, state, among others. They live in its environment, which builds a „technosystem" that creates conditions for their development or stagnation.

Around 1400, China was the world's most advanced technical civilization. China's technology was a thousand and a half or two thousand years ahead of the other technologies of the world: the blast furnace, the water clock, the iron plow, the movable loom, the compass, the jonka, the invention of gunpowder, acupuncture, paper, and printing are just some of the advances in Chinese technology. After 1400, the Chinese state lost interest in new technologies. The rulers were afraid of the destructive influence of new technologies on society. China closed itself off from the world, and contact with foreigners,

1 M. Castells, *Społeczeństwo sieci*, Warszawa 2011, p. 68.
2 Ibidem.
3 Ibidem, p. 69.
4 *Pojęcia stosowane w statystyce publicznej*, https://stat.gov.pl/metainformacje/slownik-pojec/pojecia-stosowane-w-statystyce publicznej/770,pojecie.html [access: 14.04.2022].

trade, exchange of ideas were considered a threat to the sovereignty of the Chinese state. The bureaucratic forces that came to power were anxious to maintain and nurture the strong position they had[5].

Today, China is the world leader in: patenting of inventions, production of energy from renewable sources, car manufacturing (in the case of electric cars, China is only surpassed by Tesla), implementation of 5G technology, online sales[6]. In areas such as nanotechnology, materials engineering, stem cell research, China can compete with the United States. The change in China's economic and business policies since the 1970s with the introduction of a market economy, opening up to trade, private ownership, redefining exports and targeting new technologies makes China's GDP now the highest in the world.

The role of the state and society in the diffusion of new technologies

State policy has also been crucial in the case of the „new technology powerhouse" that Japan is today. The political change that took place in Japan made it possible to make a leap in this field. Japan began to bet on foreign specialists, machinery, equipment, and use various mechanisms to increase the technological potential of the state[7]. New technologies, information technologies cannot be separated from society, just as society cannot be separated from the state. The mutual interaction of these worlds causes the release of technological potential, which, under the patronage of the state, controls the flow of technology into society, demonstrating its technological-absorptive capacity[8] and digital competence understood as the acquisition of skills (instrumental, operational) to use computer equipment [9].

5 M. Castells, op. cit., p. 49–51.

6 M. Jacoby, *Chiny innowacyjne – mocarstwo wiedzy*, https://wszechnica.org.pl/wyklad/chiny-innowacyjne-mocarstwo-wiedzy/ [access: 2.05.2022].

7 E. Bendyk, *Nowe technologie w Chinach*, https://www.polityka.pl/tygodnikpolityka/swiat/1503996,1,nowe-technologie-w-chinach.read [access: 2.05.2022].

8 M. Castells, op. cit., p. 53.

9 J. van Dijk, *Ewolucja wykluczenia cyfrowego. Od dostępu po kompetencje i użytkowanie* [in:]: *Wykluczenie społeczne. Diagnoza, wymiary i kierunki badań*, eds. M. Pokrzywa, S. Wilk, Rzeszów 2013, p. 219.

The invention of the microprocessor in Silicon Valley in 1971 ushered in the third industrial revolution, the technological revolution[10]. At that time, it was not yet realized the social, cultural, economic, economic, educational changes, among others, that the technological revolution would bring and the rate of its diffusion. All revolutions were characterized by the parameters of information and knowledge in varying degrees, starting with the development of existing knowledge through the institutionalization of this knowledge in emerging research and development laboratories, to its application to „the generation of new knowledge and information processing/communication devices, coupled in a cumulative, feedback interaction between innovation and its use"[11]. The dynamics of the development of new technologies and their absorption in society at an average level of more than 90% does not end the discovery of their impact on social life. Pandemic situations clearly show that information technologies have avoided global paralysis. To what extent they will penetrate permanently and what social impact this will have, it will be possible to assess in the field of newly undertaken research.

The development of new technologies may also influence the redefinition of already existing concepts, or the creation of completely new ones. Jerzy S. Nowak states 30[12] definitions of the information society (IS), drawn from various sources and periods. Digital technologies are now „part of our being in the world, our Mitwelt, which is obvious if we consider the importance of social media, but are also part of our Umwelt (Internet of Things, smart cities and Selbstwelt (quantified self, etc.)"[13]. Not only does the use of technology create opportunities, but it also creates consequences. As Lech Zacher writes: „the technical revolution (or, more precisely, the scientific and technological revolution) determines the direction, development trends, applications, forces appropriate policies and behaviors of governments, business and citizens"[14]. This sentence is one of the key summaries of the technical revolution. Paraphrasing this sentence after Marshall McLuhan, one can repeat that

10 M. Castells, op. cit., p. 68.
11 Ibidem, p. 69.
12 J.S. Nowak, *Społeczeństwo informacyjne – geneza i definicje* [in:] *Społeczeństwo informacyjne. Krok naprzód, dwa kroki wstecz*, eds. P. Sienkiewicz, S.J. Nowak, Katowice 2008.
13 A. Romele, *The End of the Virtual? A Hermeneutical Approach to Digitality* [in:] *Conceiving Virtuality: From Art To Technology*, ed. J. Braga, New York 2019, p. 172.
14 L.W. Zacher, *Rewolucja informacyjna a dystrybucja wiedzy i władzy. Rewolucja informacyjna a kryzys intelektualny*, Warszawa 2015, p. 77.

first we give form to our tools ”and then they shape us”[15]. Jean Baudrillard goes much further in his formulations by asking, „Am I finally a man or a machine? Today there is no longer an answer to this question: realistically and subjectively I am a man, but virtually and from a practical point of view I am a machine. Consequently, a state of anthropological uncertainty is created”[16]. The problem of anthropological uncertainty is also pointed out by Polish sociologist Zygmunt Bauman[17].

The persistent state of ignorance or limited knowledge about the new technologies, about the possibilities of their use, but also about the threats and fears caused by them, which, as John Naisbitt writes: „like the omnipotent wrath of God, the stumbling blocks of computer technology will threaten to bring complete chaos into our lives – planes will start falling from the sky, missiles will be fired without any control”[18], may limit their diffusion.

In 1184 BC the smoke telegraph was used to announce the fall of Troy, in 450 BC in Greece messages were read out using torch signals. The beginning of the 20th century was the era of telegraphs: acoustic, optical, needle, until 1876 when the telephone was invented. The development of the ARPAnet computer network took place around 1968, and in 1990 Poland was included in the European EARN network[19] opening the way to the spread of the Internet. Since then, the development of this medium and its impact on society, mainly due to its very rapid diffusion compared to other innovations, has been growing. The Internet is finding more and more applications leading researchers to formulate metaphors and comparisons of the Internet to „the human mind, and on a micro scale even the universe”[20]. Internet generating

15 M. McLuhan, *Zrozumieć media. Przedłużenia człowieka*, Warszawa 2004, p. 17.

16 J. Baudrillard, *Świat wideo i podmiot fraktalny* [in:]: *Po kinie? Audiowizualność w epoce przekaźników elektronicznych*, Kraków 1994, s. 254.

17 W. Kmiecikowski, *Niepewność – zasadnicza kategoria etyczno-antropologiczna w refleksji Zygmunta Baumana*, „Filozofia Chrześcijańska” 2011, no. 8.

18 J. Naisbitt, D. Philips, *High Tech – high touch. Technology and Our Search for Meaning*, Poznań 2003, s. 18.

19 T. Hofmhol, *Globalne społeczeństwo informacyjne – globalna rewolucja* [in:] *Społeczeństwo informacyjne: doświadczenie i przyszłość*, eds. G. Bliźniuk, J.S. Nowak, Katowice 2006, s. 48.

20 A. Betlej, *Peril and Promise of InternetTechnology for Future Social Order* [in:] *Technology, Society and Sustainability Selected Concepts, Issues and Cases*, ed. L.W. Zacher, Cham 2017, s. 120.

„a new, additional social space: cyberspace"[21]. It blurs the boundaries of space and time, generating new concepts, new social behaviors, and triggers new thought processes.

Cyber security from the perspective of its users

New technologies are also generating threats with financial estimates ranging from $445 billion to $608 billion[22].To fight with these threatscomes cyber security understood as: "the security of information networks or systems, or otherwise known as information and communications security, is the resilience of information and communications systems to threats that violate the basic information security attributes associated with information processing by information systems"[23], having in its original assumptions the mitigation of risks of digitization of social life. This prevention has been firmly established in normative acts, strategies and policies relating to the national cybersecurity system[24], with the Ministry of Digitization as the main initiator and implementer of this strategic goal.

Related to the definition of cybersecurity is the concept of cyberspace, which is defined by the U.S. Department of Defense as: „the global domain of the information environment, consisting of interdependent networks formed by information technology infrastructure and the data contained therein, including the Internet, telecommunications networks, computer

21 L. Zacher, *Technologization of Man and Marketization of His Activities and Culture of the Future* [in:] ibidem, s. 28.

22 J. Krawiec, *Cyberbezpieczeństwo. Podejście systemowe*, Warszawa 2019, p. 11.

23 Ibidem, p. 11.

24 Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018, poz. 1560; Rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych, ibidem, poz. 1806; Rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny, ibidem, poz. 2180; Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, ibidem 2019, poz. 1037; Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Dz. Urz. UE 2016, L 194/I); *Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej*, Warszawa 2013.

systems, and embedded processors and controllers"[25]. Both cybersecurity and cyberspace have received many definitions not only on the national, but also on the international level. These concepts have been created not only by cybersecurity specialists, researchers, but also by normative acts and strategic documents from this area creating cyber security policy.

Information security policy is defined as: „a set of laws, rules and experiences that establish how sensitive information is managed, protected, and distributed within a defined system"[26]. While determining the security level of information systems, it refers to the security level of the weakest link in the system[27]. A 2017 survey of senior managers found 69% confirmed the need to redefine legacy security policies[28]. Such a result is a derivative of the rapid diffusion of new technologies, which thanks to the fast dynamics of development generate a different kind of threats than those covered in the existing IT security policies.

The concept of cybersecurity can also be found in relation to medical devices (pacemakers, defibrillators, insulin pumps), observing for about 10 years disturbing attempts by hackers to break into the systems that monitor these devices[29], which supports the thesis that such threats apply to any device connected to the Internet.

Information warfare is also becoming increasingly important as one of hybrid warfare. It is one of the key non-military capabilities of armies, which, by introducing disinformation, destabilizes forces, hinders communication, manipulates human moods, and weakens the will to fight. The current situation of the war in Ukraine has highlighted this aspect of cyberspace by showing Russia's information cyberattacks. Yannick Harrel recognizes that

25 Z. Chmielewski, *Polityka publiczna w zakresie ochrony cyberprzestrzeni w UE i państwach członkowskich*, „Studia z Polityki Publicznej" 2016, vol. 10, no. 2, p. 105.

26 I. Oleksiewicz, *Ochrona cyberprzestrzeni Unii Europejskiej. Polityka – Strategia – Prawo*, Warszawa 2021, p. 22.

27 Ibidem, s. 22.

28 L. Ling i in., *Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior*, „International Journal of Information Management" 2018, vol. 45, p. 13–24.

29 A. Baranchuk i in., *Cybersecurity for Cardiac Implantable Electronic Devices: What Should You Know?*, „Journal of the American College of Cardiology" 2018, vol. 71, no. 11, p. 1284–1288.

„[...] cyberspace allows the use of relative discretion, enables rapid or delayed strikes, synchronous or asynchronous actions that weaken enemy forces"[30].

The resilience of information systems to threats is strengthened by an extensive national cyber security system. However, a large role in reducing the risks associated with security breaches of these systems is the awareness of the users themselves. In the area of cyber security, under the heading of cyber hygiene[31] introduced some informal catalog of actions and behaviors that should alert users of information systems to threats. „Microsoft data shows that using multi-factor authentication reduces vulnerability to identity-based attacks (it's all about impersonation) by 99 percent"[32]. Taking often simple actions such as: logging in with biometrics, not opening files or „not clicking" on links from unknown people, installing anti-virus software, and keeping software up to date are just some of the firewalls against cyber attack.

Cyberhygiene principles are security principles: „in the catalog of social needs, ensuring security occupies a high position. It can even be said that it is one of the basic human needs that allows for an undisturbed existence"[33]. This assertion reinforces the essence of cyberhygiene and prompts us to structure it into: a secure work environment, responsible use of Internet access, use of reliable service providers, making identity theft more difficult by, for example, using unique passwords and two-factor authentication, not sending scans of identity documents. However, it is important to be aware that data theft incidents do occur. The Have I Been Pwned portal „collected data on 368 cases of theft of large personal databases. According to the statistics of the Office of Protection of Personal Data (UODO), in the first year of implementation of the RODO, over 4.5 thousand violations of personal data protection were reported to the authority"[34]. This may indicate, not so much an increase in such breaches with respect to the past, but the fact that we have consciously begun to use the instruments of RODO.

30 S. Gardocki, J. Worona, *Wykorzystanie przez Rosję cyberprzestrzeni w konfliktach hybrydowych a rosyjska polityka cyberbezpieczeństwa*, „Colloquium Wydziału Nauk Humanistycznych i Społecznych AMW" 2020, vol. 12, no. 2, p. 33–46.

31 *Cyberhigiena, czyli dobre nawyki, które ochronią nas przed hakerami i utratą cyfrowej tożsamości*, https://spidersweb.pl/bizblog/cyberhigiena-cyfrowa-tozsamosc/ [access: 1.06.2022].

32 Ibidem.

33 M. Karpiuk, *Position of the Local Government of Commune Level in the Space of Security and Public Order*, „Studia Iuridica Lublinensia" 2019, no. 2, p. 28.

34 *Cyberbezpieczeństwo*, eds. C. Banasiński, M. Rojszczak, Warszawa 2020, p. 44–52.

Conclusion

New technologies are undoubtedly an attribute of modern society. Penetrating many areas of our lives, they automate and streamline many processes. They activate national and international activities, creating new cooperation networks. They generate hitherto unknown threats, which can be prevented. As users of information systems we should care about raising our awareness in the area of cyber security. Campaigns prepared also on the level of governmental organizations, such as „For everyone – cyberhygiene", which in short films (How to safely navigate the network? Who's talking?, Spoofing and phishing, Safe passwords – everything you always wanted to know, Risky online behavior of children, etc.), which show the mechanisms to prevent a cyber attack, as it is possible from the position of a direct user of information systems. These two areas of new technologies and cyber security are areas that for dynamic development require not only state intervention, but also a society aware of development opportunities and threats. The development of new technologies will generate new, previously unknown threats and stimulate the development of tools to ensure secure cyberspace.

Bibliography

Baranchuk A. i in., *Cybersecurity for Cardiac Implantable Electronic Devices: What Should You Know?*, „Journal of the American College of Cardiology" 2018, vol. 71, no. 11.

Baudrillard J., *Świat wideo i podmiot fraktalny* [in:]: *Po kinie? Audiowizualność w epoce przekaźników elektronicznych*, Kraków 1994.

Bendyk E., *Nowe technologie w Chinach*, https://www.polityka.pl/tygodnikpolityka/swiat/1503996,1,nowe-technologie-w-chinach.read [access: 2.05.2022].

Castells M., *Społeczeństwo sieci*, Warszawa 2011.

Chmielewski Z., *Polityka publiczna w zakresie ochrony cyberprzestrzeni w UE i państwach członkowskich*, „Studia z Polityki Publicznej" 2016, vol. 10, no. 2.

Cyberbezpieczeństwo, eds. C. Banasiński, M. Rojszczak, Warszawa 2020.

Cyberhigiena, czyli dobre nawyki, które ochronią nas przed hakerami i utratą cyfrowej tożsamości, https://spidersweb.pl/bizblog/cyberhigiena-cyfrowa-tozsamosc/ [access: 1.06.2022].

Dijk J., van, *Ewolucja wykluczenia cyfrowego. Od dostępu po kompetencje i użytkowanie* [in:]: *Wykluczenie społeczne. Diagnoza, wymiary i kierunki badań*, eds. M. Pokrzywa, S. Wilk, Rzeszów 2013.

Gardocki S., Worona J., *Wykorzystanie przez Rosję cyberprzestrzeni w konfliktach hybrydowych a rosyjska polityka cyberbezpieczeństwa*, „Colloquium Wydziału Nauk Humanistycznych i Społecznych AMW" 2020, vol. 12, no. 2.

Hofmhol T., *Globalne społeczeństwo informacyjne – globalna rewolucja* [in:] *Społeczeństwo informacyjne: doświadczenie i przyszłość*, eds. G. Bliźniuk, J.S. Nowak, Katowice 2006.

Jacoby M., *Chiny innowacyjne – mocarstwo wiedzy*, https://wszechnica.org.pl/wyklad/chiny-innowacyjne-mocarstwo-wiedzy/ [access: 2.05.2022].

Karpiuk M., *Position of the Local Government of Commune Level in the Space of Security and Public Order*, „Studia Iuridica Lublinensia" 2019, no. 2.

Kmiecikowski W., *Niepewność - zasadnicza kategoria etyczno-antropologiczna w refleksji Zygmunta Baumana*, „Filozofia Chrześcijańska" 2011, nr 8.
Krawiec J., *Cyberbezpieczeństwo. Podejście systemowe*, Warszawa 2019.
Ling L. i in., *Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior*, „International Journal of Information Management" 2018, vol. 45.
McLuhan M., *Zrozumieć media. Przedłużenia człowieka*, Warszawa 2004.
Naisbitt J., Philips D., *High Tech – high touch. Technology and Our Search for Meaning*, Poznań 2003.
Nowak J.S., *Społeczeństwo informacyjne – geneza i definicje* [w:] *Społeczeństwo informacyjne. Krok naprzód, dwa kroki wstecz*, eds. P. Sienkiewicz, S.J. Nowak, Katowice 2008.
Oleksiewicz I., *Ochrona cyberprzestrzeni Unii Europejskiej. Polityka – Strategia – Prawo*, Warszawa 2021.
Pojęcia stosowane w statystyce publicznej, https://stat.gov.pl/metainformacje/slownik-pojec/pojecia-stosowane-w-statystyce publicznej/770,pojecie.html [access: 14.04.2022].
Romele A., *The End of the Virtual? A Hermeneutical Approach to Digitality* [in:] *Conceiving Virtuality: From Art To Technology*, ed. J. Braga, New York 2019.
Technology, Society and Sustainability Selected Concepts, Issues and Cases, ed. L.W. Zacher, Cham 2017.
Zacher L.W., *Rewolucja informacyjna a dystrybucja wiedzy i władzy. Rewolucja informacyjna a kryzys intelektualny*, Warszawa 2015.

Cyberbezpieczeństwo z punktu widzenia użytkownika nowych technologii

Streszczenie

Nowe technologie to w świecie postępujących procesów globalizacji, rewolucji naukowo-technicznej jeden z najważniejszych wskaźników służących projektowaniu wielu obszarów życia społecznego. Wykorzystanie technologii informacyjnych zapoczątkowało wiele zjawisk społecznych, generując wiele dotąd nieznanych pojęć, zagrożeń, a w odpowiedzi – nowych obszarów zainteresowań eksperckich i badawczych. Jednym z nich jest cyberbezpieczeństwo, które główny nacisk kładzie na budowanie krajowych, europejskich czy międzynarodowych polityk zabezpieczających funkcjonowanie systemów informacyjnych.

Celem niniejszej pracy jest analiza i ocena cyberbezpieczeństwa z punktu widzenia użytkownika nowych technologii. W badaniach zastosowano metodę syntetyczo-analityczną analizy literatury krajowej i zagranicznej z dziedziny nowych technologii i cyberbezpieczeństwa.

Słowa kluczowe: cyberbezpieczeństwo, cyberhigiena, nowe technologie, technologie informacyjne, technologie cyfrowe