Krzysztof Kaczmarek*

Vulnerability to Cyber Threats: A Qualitative Analysis From Societal and Institutional Perspectives

Abstract

With the rapid development of ICT and the shifting of much of social activity online, countering cyber threats has become a challenge both for individuals and governments. The research hypothesis is that the number and type of cyber attacks are directly related to an individual's vulnerability to cyber threats. In order to verify this hypothesis, quantitative and qualitative methods, literature survey and the desk research method were used.

The analyses conducted by the Author explicitly indicated that what is the weakest element in a cyber security system is the human factor. At the same time, it is fatigue and routine that are the worst enemies, even for a cyber security professional. One way to increase the level of security is to assume that every time a network service is used, it may carry the risk of a cyber attack with consequences that are difficult to predict. This allows for vigilance even in everyday activities that require access to the network.

Key words: digital society, technological progress, vulnerability to cyber threats, security of institutions

* Krzysztof Kaczmarek, PhD, Faculty of Humanities, Koszalin University of Technology, e-mail: puola@tlen.pl; ORCID: 0000-0001-8519-1667.

Introduction

A great portion of the activity of modern societies takes place in cyberspace. This includes work, learning, social interaction, private life and social services. However, unlawful behaviour and violations of social norms can be observed in every society. This type of activity also takes place online. The rapid development of Information and Communications Technology (ICT) is making the use of digital tools increasingly easy and intuitive even for people without the knowledge of how digital reality functions. Nowadays, being a member of a digital and information society does not necessarily mean being familiar with the principles which it is based on. This state of affairs is exploited not only by criminals but also by states or organisations linked to them, in order to influence public behaviour or launch cyber attacks on critical infrastructure which proper functioning of states depends on[1]. At the same time, it should be noted that cyber disruptions can have a negative impact on the delivery of critical services[2]. In the event of disruption to telecommunications networks caused by a cyber attack, cashless payments, a significant proportion of medical services, administration, traffic control systems or electricity grid control systems cease to function[3]. This, in turn, could cause a chain reaction with consequences that are difficult to predict.

Advances in ICT are also causing qualitative changes in the labour market. This became evident during the COVID-19 pandemic, when demand for certain professions disappeared while new ones emerged[4].

When analysing cyber attacks, both quantitatively and qualitatively, it is important to take into account that cyberspace has no control barriers[5]. In a sense, this is an entity that is abstract for humans, yet one that has a real impact on the reality which societies and states function in. In this context, cyber attacks can be carried out from anywhere in the world against any target. It is

[1] M. Karpiuk, *Crisis management vs. cyber threat*, „Sicurezza, Terrorismo e Società" 2022, no. 2, p. 121.

[2] M. Czuryk, *The Legal Status of Digital Service Providers in The National Cybersecurity system*, „Cybersecurity and Law" 2024, no. 1, p. 40.

[3] M. Czuryk, *Cybersecurity and Protection of Critical Infrastructure*, „Studia Iuridica Lublinensia" 2023, no. 5, p. 50.

[4] E. Włodyka, *Dlaczego potrzebujemy e-administracji? Rozwój podstawowych umiejętności cyfrowych pracowników administracji na Pomorzu Zachodnim*, „Acta Politica Polonica" 2021, no 2, p. 91.

[5] M. Karpiuk, *Cybersecurity as an element in the planning activities of public administration*, „Cybersecurity and Law" 2021, no. 1, p. 50.

also to be emphasised that the use of network services at a particular location in no way determines the physical location of the data used and processed.

In the context of research into cyber threats, it seems relevant that the digital world is a phenomenon that is completely new to humanity. Consequently, there is not, because there cannot be, any tradition of passing on knowledge in this area from generation to generation. At the same time, the pace of technological progress means that research and analyses in this area must be carried out on a continuous basis and knowledge updated almost daily. It should be emphasised at this point that it is prevention that constitutes one of the most crucial elements of ensuring security (including cyber security)[6]. However, in order to be able to counter threats effectively, it is necessary to possess knowledge that allows one to predict hostile actions with a high degree of probability, while also taking into account that even little likely events are not impossible. This knowledge can be gained from analyses of previous phenomena and events, which allows rapid action to be taken and to prevent serious consequences of a cyber attack[7].

The aim of the present article is to examine the vulnerability of individuals and institutions to cyber attacks: both qualitatively and quantitatively. The research results will allow predictions of future trends in this area. The research hypothesis is that the number and type of cyber attacks are directly related to an individual's vulnerability to cyber threats. Quantitative and qualitative methods, literature survey and the desk research method will be employed to verify this hypothesis.

Cyber threats in the context of the proper functioning of societies and states

Adequate functioning of contemporary societies and countries relies on seamless access to online services, and digital competence is one of the most important determinants of the quality of life[8]. At the same time, highly

[6] M. Czuryk, *Activities of the Local Government During a State of Natural Disaster*, „Studia Iuridica Lublinensia" 2021, no. 4, p. 122.

[7] M. Karpiuk, *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, no. 2, p. 63.

[8] A. Bencsik, M. Karpiuk, N. Strizzolo, *Information Society Services and Their Cybersecurity*, ibidem 2024, no. 1, p. 259.

digitalised societies are highly vulnerable to cyber attacks, and criminals perpetrating those attacks may exploit the lack of awareness of possible cyber threats among those using ICT tools[9]. Previous experience of numerous attack incidents, including hacks and data breaches, indicates that cyber security has become an extremely important area of research[10].

In the context of cyber-security and cyber-attack research, it is of a great significance that for technologically developed countries, cyber attacks can destabilise the functioning of public authorities[11]. At the same time, because of this, security in cyberspace possesses also a military context[12], and the military aspects of cyber security is one of NATO's defence priorities[13]. Therefore, protection against cyber threats should constitute a priority area of state policy[14].

Another threat, resulting from the development of ICT, is a widespread exposure to disinformation. It is now impossible to verify the veracity of information on one's own, and videos or statements found in cyberspace can under no circumstances be assumed to be true without prior verification[15]. Even economically and militarily strong democratic states do not possess any effective tools to combat this phenomenon, and their preventive action consists only in information and education campaigns[16].

One purpose of cyber attacks is to gain unauthorised access to information and data, including personal data, which can be used to commit further crimes. One of the institutions tasked with ensuring cyber security is local government[17]. In this case, it should be noted that the local authority manages

[9] M. Karpiuk, W. Pizło, K. Kaczmarek, *Cybersecurity Management – Current State and Directions of Change*, „International Journal of Legal Studies" 2023, no. 2, p. 647.

[10] O. Evsyukova, M. Karpiuk, M. Kelemen, *Cyberthreats in Ukraine, Poland and Slovakia*, „Cybersecurity and Law" 2024, no. 1, p. 75.

[11] A. Bencsik, M. Karpiuk, M. Kelemen, E. Włodyka, *Cybersecurity in the Visegrad Group Countries*, Maribor 2023, p. 1.

[12] A. Bencsik, M. Karpiuk, *The legal status of the cyberarmy in Hungary and Poland. An overview*, „Cybersecurity and Law" 2023, no. 2, p. 28.

[13] Eidem, *Cybersecurity in Hungary and Poland. Military aspects*, ibidem 2023, no. 1, p. 85.

[14] M. Karpiuk, M. Kelemen, *Cybersecurity in civil aviation in Poland and Slovakia*, ibidem 2022, no. 2, p. 71.

[15] K. Kaczmarek, *Technologia deep fake jako potencjalne narzędzie wpływania na decyzje wyborcze w państwach byłego bloku wschodniego* [in:] *Cyberbezpieczeństwo. Aspekty krajowe i międzynarodowe*, ed. M. Karpiuk, Warszawa 2024, p. 61.

[16] K. Wasilewski, *Fake News and the Europeanization of Cyberspace*, „Polish Political Science Yearbook" 2021, no. 4, p. 9.

[17] I. Hoffman, M. Karpiuk, *The local self-government's place in the cybersecurity domain. Examples of Poland and Hungary*, „Cybersecurity and Law" 2022, no. 1, p. 174.

the precise personal data of citizens[18]. However, it should be emphasised that as regards protection of personal data, it is user awareness and knowledge of how to protect this data that is of key importance[19].

In the case of democratic states, cyber threats also affect the conduct of elections. What is the most serious threat is the possibility of external interference not only in the electoral process but also in the accuracy of vote counting[20].

With the economy entering the era of Industry 4.0 and the digital revolution of societies, digitisation processes also have an increasing presence in public administration[21]. At the same time, as in other areas of social life, artificial intelligence (AI) is finding more and more applications in public administration[22]. Meanwhile, AI is, although being the most technologically advanced tool, only a tool whose use depends solely on its maker and user. It is currently impossible to determine what risks its misuse or irresponsible use may bring. One can only assume that AI tools will increasingly be produced and used by criminals.

To conclude this part of the article, it is important to emphasise that digitisation processes affect almost every aspect of private, social, professional and political life. Information and communication technologies affect everyone and every area of their lives[23]. As a result, everyone is permanently exposed to cyber attacks or their consequences. This is particularly true for residents of Europe, which ranked as the most frequently attacked region in 2023, experiencing 32% of global cyber incidents[24].

[18] E.M. Włodyka, *Gotowi – do startu – start? Przyczynek do dyskusji nad gotowością jednostek samorządu terytorialnego do zapewniania cyberbezpieczeństwa*, ibidem, p. 218.

[19] C. Melchior, U. Soler, *Security of Personal Data in Cyberspace in the Opinion of Students of the University of Udine*, ibidem 2024, no. 1, p. 229.

[20] E.M. Włodyka, *Polaryzacja, kohabitacja czy integracja? Wyzwania cyberbezpieczeństwa procesów wyborczych w Polsce* [in:] *Cyberbezpieczeństwo. Aspekty...*, p. 116.

[21] Eadem, *Dostępność cyfrowa w Unii Europejskiej – praktyka i założenia teoretyczne*, „Rocznik Integracji Europejskiej” 2022, no. 16, p. 356.

[22] Eadem, *Sztuczna inteligencja w sektorze publicznym – stan i oczekiwania* [in:] *Edukacja, komunikacja i dyskursy społeczne. Studia humanistyczne i społeczne*, eds. L.J. Maksymowicz, Z. Danielewicz, Koszalin 2023, p. 123.

[23] U. Soler, *Technologie sieciowe vs. terroryzm – czy mogą być społecznie szkodliwe?*, „Zeszyty Naukowe. Organizacja i Zarządzanie” 2015, no. 85, p. 503.

[24] S. Kaczmarek, *Blisko ⅓ światowych cyberataków była w 2023 r. wymierzona w Europę*, 2024, https://www.telko.in/blisko-1-3-swiatowych-cyberatakow-byla-w-2023-r-wymierzona-w-europe [access: 24.03.2024].

Causes of vulnerability to cyber attacks

Vulnerability to cyber attacks can most generally be divided into two types. The first one is technical holes and security flaws, while the second one is due to human error. However, the two types are not independent of each other. It is frequently that technical deficiencies are the result of the system user's activity. This is most frequently due to a lack of awareness or ignoring the reality of threats and potential consequences of successful attacks.

Generally speaking, the most common cause of successful attacks is the victim's blatant mistakes, resulting from a lack of basic hygiene in the safe use of digital services[25]. For example, even users of highly secured institutional systems are vulnerable to cyber attacks. It is not infrequent that cybercriminals prepare malware and effectively deliver it to users of an organisation using its own email system, bypassing all security[26]. In such a case, the infection of the device used by the system user may lead to serious breaches in the entire system. From the perspective of public and national security, the greatest threat may arise when a device used by a person with access to classified information is infected. This does not only concern unauthorised access to this information but also acquisition of control over e.g. systems supporting emergency management.

There is currently a significant increase both in the variety and number of cyber attacks and their consequences in the cyber security landscape. Consequently, the ways of preventing these must also constantly change. This is stated, among other things, in the *Enisa Threat Landscape 2023* report prepared by the EU Agency for Cybersecurity (ENISA)[27].

One of the elementary security enhancements recommended by IT professionals is the use of strong, unique and hard-to-crack passwords. However, in recent years, the effectiveness of this form of security has been declining[28]. Various forms of biometrics are becoming an alternative, such as iris, face and fingerprint scanning as well as push notifications, text messages

[25] N. Przybylska, *Cyberatak to kwestia czasu. „Ogromne pieniądze kradzione są w niezwykle trudny do wyśledzenia sposób"*, 2022, https://businessinsider.com.pl/technologie/digital-poland/przyczyna-udanego-cyberataku-sa-razace-bledy-ofiary/zlv37hj [access: 24.03.2024].

[26] Ibidem.

[27] *ENISA Threat Landscape 2023*, 2023, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023/@@download/fullReport [access: 24.03.2024].

[28] M. Marszycki, *Czy pożegnamy się ze stosowaniem haseł?*, 2024, https://itwiz.pl/czy-pozegnamy-sie-ze-stosowaniem-hasel/ [access: 24.03.2024].

with one-time pins, QR codes and USB security keys[29]. However, it is important to note that even the most technologically advanced cyber security tools are only used to the extent that they are implemented by their users. It is just as often the case that in an institution, an implementation of cyber security procedures only takes place when significant losses have been incurred as a result of a cyber attack. Indeed, the provision of cyber security can never be a one-off project with a defined beginning and end. At the same time, in the case of a cyber security chain, the system is only as resilient as its weakest link. Thus, in the case of an institution, every element, even seemingly the least significant one, that can affect the entire system must always be taken into account.

Cyber risks must form part of an organisation's daily risk management. The same risk management principles apply to cyber risk management as to other risks. They should take into account the fact that cyber security solutions and technologies are developing so rapidly that there is always a danger of using outdated methods to assess cyber risks. In this case, obsolete methods are to be understood as those that have been in use for a period of time allowing for the development of newer cyber attack methods[30]. Thus, it may be that a method implemented only a few days earlier is considered obsolete.

With the increasing threat of attacks, it is the human factor that plays a key role in cyber security. This is most often due to: 1) exaggerating the risk of spectacular but relatively rare incidents and downplaying the risk of common but less spectacular incidents; 2) difficulty in estimating the risk of those incidents that deviate from everyday situations; 3) overestimating the risk associated with the actions of a specific individual and underestimating the risk associated with the actions of anonymous people; 4) overstating the risks associated with uncontrollable situations and understating the risks of those actions that are willingly taken; 5) overestimating the risks of incidents that are publicly discussed[31]. Ignoring cyber threats also stems from the belief that negative events, including the effects of cyber attacks, most often affect others[32].

[29] Ibidem.

[30] *Kyberturvallisuus ja yrityksen hallituksen vastuu*, p. 15, https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf [access: 24.03.2024].

[31] *Psychologiczne aspekty cyberbezpieczeństwa*, https://cyberpolicy.nask.pl/psychologiczne-aspekty-cyberbezpieczenstwa/ [access: 24.03.2024].

[32] Ibidem.

Conclusions

The analyses conducted in this article have clearly indicated that the human factor is the weakest element in the cyber security system. The research hypothesis assuming that the number and type of cyber attacks are directly related to an individual's vulnerability to cyber threats was also positively verified.

This state of affairs is due to humanity's evolutionary maladaptation to functioning in information noise and in the digital world. Technological progress is so rapid that even expert knowledge becomes obsolete in a relatively short period of time. It is also important to bear in mind that there is an arms race in cyberspace, both in terms of international tensions and in terms of cybercrime and ways to combat it. It is also to be noted that one's own cyber security should first and foremost be taken care of by oneself. The global security environment must also be taken into account when taking appropriate measures to increase the level of online security. Currently, in conducting hybrid operations against the countries of the Euro-Atlantic community, Russia is using the following tools on an unprecedented scale: disinformation, manipulation, fake news, information disruption, cyber attacks and cyber espionage[33].

The problem for many organisations is the effectiveness of the perception of warning signals, which manifests itself most frequently in the failure to spot important signals in time and, as a result, a lack of adequate preparation for the occurrence of negative incidents. The consequences of this are so-called surprises consisting of the sudden appearance of a cascade of negative events, ones of high intensity and causing significant losses, posing a threat of a degradation of the organisation. At the same time, it is clear after the fact that there were warning signals before that[34].

In conclusion, it should be emphasised that research on cyber security should be holistic and include all possible factors that have or could have an impact on this area, even if not yet present. When working on cyber security

[33] T. Nowak, *Budowa odporności na obecne i przyszłe zagrożenia o charakterze hybrydowym. Rekomendacje dla Polski*, „Roczniki Nauk Społecznych" 2022, no. 4, p. 44.

[34] B. Ćwik, *Postrzeganie zagrożeń w systemach bezpieczeństwa organizacji*, „Modern Management Review" 2017, no. 3, p. 28. See also: idem, *Postrzeganie sygnałów ostrzegających organizację w sytuacjach niedeterministycznych*, Warszawa 2023; idem, *Multidisciplinary approach to the analysis of the process of perceiving warning signals*, „Security and Defence Quarterly" 2017, no. 2.

strategies, in addition to IT specialists, experts from various fields such as psychology, sociology, mathematics or even history should be involved.

In the case of cyber security, continuous education in this area appears to be necessary. At the same time, the level of security can be increased with the assumption that every use of network services involves a potential risk. This allows one to stay on alert in all situations. After all, it needs to be remembered that it is fatigue and routine that is the worst enemy even for a cyber security professional. Meanwhile, even one-off risky behaviour may have consequences that are difficult to predict.

Bibliography

Bencsik A., Karpiuk M., *Cybersecurity in Hungary and Poland. Military aspects*, „Cybersecurity and Law" 2023, no. 1.

Bencsik A., Karpiuk M., *The legal status of the cyberarmy in Hungary and Poland. An overview*, „Cybersecurity and Law" 2023, no. 2.

Bencsik A., Karpiuk M., Kelemen M., Włodyka E., *Cybersecurity in the Visegrad Group Countries*, Maribor 2023.

Bencsik A., Karpiuk M., Strizzolo N., *Information Society Services and Their Cybersecurity*, „Cybersecurity and Law" 2024, no. 1.

Czuryk M., *Activities of the Local Government During a State of Natural Disaster*, „Studia Iuridica Lublinensia" 2021, no. 4.

Czuryk M., *Cybersecurity and Protection of Critical Infrastructure*, „Studia Iuridica Lublinensia" 2023, no. 5.

Czuryk M., *The Legal Status of Digital Service Providers in The National Cybersecurity System*, „Cybersecurity and Law" 2024, no. 1.

Ćwik B., *Multidisciplinary approach to the analysis of the process of perceiving warning signals*, „Security and Defence Quarterly" 2017, no. 2.

Ćwik B., *Postrzeganie sygnałów ostrzegających organizację w sytuacjach niedeterministycznych*, Warszawa 2023.

Ćwik B., *Postrzeganie zagrożeń w systemach bezpieczeństwa organizacji*, „Modern Management Review" 2017, no. 3.

ENISA Threat Landscape 2023, 2023, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023/@@download/fullReport [access: 24.03.2024].

Evsyukova O., Karpiuk M., Kelemen M., *Cyberthreats in Ukraine, Poland and Slovakia*, „Cybersecurity and Law" 2024, no. 1.

Hoffman I., Karpiuk M., *The local self-government's place in the cybersecurity domain. Examples of Poland and Hungary*, „Cybersecurity and Law" 2022, no. 1.

Kaczmarek K., *Technologia deep fake jako potencjalne narzędzie wpływania na decyzje wyborcze w państwach byłego bloku wschodniego* [in:] *Cyberbezpieczeństwo. Aspekty krajowe i międzynarodowe*, ed. M. Karpiuk, Warszawa 2024.

Kaczmarek S., *Blisko ⅓ światowych cyberataków była w 2023 r. wymierzona w Europę*, 2024, https://www.telko.in/blisko-1-3-swiatowych-cyberatakow-byla-w-2023-r-wymierzona-w-europe [access: 24.03.2024].

Karpiuk M., *Crisis management vs. cyber threat*, „Sicurezza, Terrorismo e società" 2022, no. 2.

Karpiuk M., *Cybersecurity as an element in the planning activities of public administration*, „Cybersecurity and Law" 2021, no. 1.

Karpiuk M., *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, no. 2.

Karpiuk M., Kelemen M., *Cybersecurity in civil aviation in Poland and Slovakia*, „Cybersecurity and Law" 2022, no. 2.

Karpiuk M., Pizło W., Kaczmarek K., *Cybersecurity Management – Current State And Directions Of Change*, "International Journal of Legal Studies" 2023, no. 2.

Kyberturvallisuus ja yrityksen hallituksen vastuu, https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf [access: 24.03.2024].

Marszycki M., *Czy pożegnamy się ze stosowaniem haseł?*, 2024, https://itwiz.pl/czy-pozegnamy-sie-ze-stosowaniem-hasel/ [access: 24.03.2024].

Melchior C., Soler U., *Security of Personal Data in Cyberspace in the Opinion of Students of the University of Udine*, „Cybersecurity and Law" 2024, no. 1.

Nowak T., *Budowa odporności na obecne i przyszłe zagrożenia o charakterze hybrydowym. Rekomendacje dla Polski*, „Roczniki Nauk Społecznych" 2022, no. 4.

Przybylska N., *Cyberatak to kwestia czasu. „Ogromne pieniądze kradzione są w niezwykle trudny do wyśledzenia sposób"*, 2022, https://businessinsider.com.pl/technologie/digital-poland/przyczyna-udanego-cyberataku-sa-razace-bledy-ofiary/zlv37hj [access: 24.03.2024].

Psychologiczne aspekty cyberbezpieczeństwa, https://cyberpolicy.nask.pl/psychologiczne-aspekty-cyberbezpieczenstwa/ [access: 24.03.2024].

Soler U., *Technologie sieciowe vs. terroryzm – czy mogą być społecznie szkodliwe?*, „Zeszyty Naukowe. Organizacja i Zarządzanie" 2015, no. 85.

Wasilewski K., *Fake News and the Europeanization of Cyberspace*, „Polish Political Science Yearbook" 2021, no. 4.

Włodyka E.M., *Dostępność cyfrowa w Unii Europejskiej – praktyka i założenia teoretyczne*, „Rocznik Integracji Europejskiej" 2022, no. 16.

Włodyka E.M., *Gotowi – do startu – start? Przyczynek do dyskusji nad gotowością jednostek samorządu terytorialnego do zapewniania cyberbezpieczeństwa*, „Cybersecurity and Law" 2022, no. 1.

Włodyka E.M., *Polaryzacja, kohabitacja czy integracja? Wyzwania cyberbezpieczeństwa procesów wyborczych w Polsce* [in:] *Cyberbezpieczeństwo. Aspekty krajowe i międzynarodowe*, ed. M. Karpiuk, Warszawa 2024.

Włodyka E.M., *Sztuczna inteligencja w sektorze publicznym – stan i oczekiwania* [in:] *Edukacja, komunikacja i dyskursy społeczne. Studia humanistyczne i społeczne*, eds. L.J. Maksymowicz, Z. Danielewicz, Koszalin 2023.

Włodyka E., *Dlaczego potrzebujemy e-administracji? Rozwój podstawowych umiejętności cyfrowych pracowników administracji na Pomorzu Zachodnim*, "Acta Politica Polonica" 2021, no 2.

Podatność na cyberzagrożenia: analiza jakościowa w ujęciu społecznym i instytucjonalnym

Streszczenie

W związku z szybkim rozwoju ICT i przeniesieniem do sieci znacznej części aktywności społecznych przeciwdziałanie cyberzagrożeniom stało się wyzwaniem zarówno dla jednostek, jaki i dla państw. Hipoteza badawcza zakłada, że liczba i rodzaje cyberataków są bezpośrednio związane z podatnością jednostki na cyberzagrożenia. W celu weryfikacji tej hipotezy zostały zastosowane metody: ilościowa, jakościowa, badanie literatury przedmiotu oraz metoda *desk research*.

Analizy przeprowadzone przez autora jednoznacznie pokazały, że najsłabszym elementem w systemie cyberbezpieczeństwa jest człowiek. Jednocześnie największym wrogiem, nawet dla osoby zajmującej się zawodowo cyberbezpieczeństwem, są zmęczenie i rutyna. Jednym ze sposobów zwiększenia poziomu bezpieczeństwa jest założenie, że każdorazowe korzystanie z usług sieciowych może nieść ze sobą ryzyko cyberataku o trudnych do przewidzenia konsekwencjach.

Słowa kluczowe: społeczeństwo cyfrowe, postęp technologiczny, podatność na cyberzagrożenia, bezpieczeństwo instytucji