S T U D I A N A D B E Z P I E C Z E Ń S T W E M

Nr 10 **s. 17–34** **2025**

ISSN 2543–7321
© Instytut Bezpieczeństwa i Socjologii,
Uniwersytet Pomorski w Słupsku
Przyjęto: 30.05.2025
Zaakceptowano: 30.05.2025

Oryginalna praca badawcza DOI: 10.34858/SNB.10.2025.002

Joanna Grubicka
Pomeranian University in Słupsk
e-mail: joanna.grubicka@upsl.edu.pl
ORCID: 0000-0001-7934-6044

CYBER THREATS AS A DETERMINANT OF RISK FOR PERSONAL SECURITY IN CYBERSPACE

CYBERZAGROŻENIA JAKO DETERMINANTA RYZYKA DLA BEZPIECZEŃSTWA PERSONALNEGO W CYBERPRZESTRZENI

Abstract: The article examines cyber threats and risk in cyberspace in the context of the personal security of modern individuals. The research problem concerns how contemporary cyber threats determine the level and nature of risk to individuals and which risk-analysis and risk-management mechanisms are most relevant to mitigating their consequences. The aim of the study is to identify and systematise the principal categories and sources of cyber threats affecting personal security, to clarify the relationship between cyber threat and risk, and to determine the significance of risk analysis, risk assessment and risk-management mechanisms for the protection of individuals in the digital environment. The study uses a qualitative theoretical and analytical approach based on critical analysis of the literature, analysis of normative and standardisation documents (including PN-I-13335-1:1999, ISO/IEC 27005:2022 and NIST SP 800-30 Rev. 1), comparative analysis, synthesis and classification. The analysis covers threats such as identity theft, phishing, cyberbullying, ransomware, social engineering, malware, privacy breaches and disinformation. The findings support the hypothesis that cyber threats are a significant determinant of personal-security risk and that effective risk reduction requires systematic assessment and an interdisciplinary combination of technical, organisational, legal and educational measures.

Zarys treści: Artykuł podejmuje problematykę cyberzagrożeń i ryzyka w cyberprzestrzeni w kontekście bezpieczeństwa personalnego współczesnego człowieka, koncentrując się na analizie pojęć zagrożenia, cyberzagrożenia oraz ryzyka i ich znaczenia dla ochrony jednostki w środowisku cyfrowym. W pracy omówiono klasyfikacje zagrożeń bezpieczeństwa informacyjnego oraz ich źródła i skutki, ze szczególnym uwzględnieniem takich zjawisk, jak: kradzież tożsamości, phishing, cyberprzemoc, ransomware, ataki socjotechniczne czy naruszenie prywatności. Wskazano na kluczową rolę analizy i oceny ryzyka jako podstawy zarządzania bezpieczeństwem i podkreślono konieczność podejścia interdyscyplinarnego. Wnioski wskazują, że skuteczna ochrona w cyberprzestrzeni wymaga identyfikacji zagrożeń, systematycznej oceny ryzyka, wdrażania strategii minimalizacji oraz rozwijania świadomości cyfrowej użytkowników.

Keywords: cyber threats, risk, cyberspace, personal security, information security, risk management.

Słowa kluczowe: cyberzagrożenia, ryzyko, cyberprzestrzeń, bezpieczeństwo personalne, bezpieczeństwo informacyjne, zarządzanie ryzykiem.

Introduction

Cyberspace is a dynamic environment in which people operate, offering numerous opportunities for development alongside increasingly complex and multifaceted threats. The security landscape in the digital environment is shaped both by technological advancements and by individuals' growing exposure to various forms of cyber threats.[1] A review of the literature on this phenomenon allows for an in-depth analysis of its characteristics and impact on the individual, whilst highlighting the diversity of interpretations resulting from the global reach and interdisciplinary nature of cyberspace. At the same time, it is worth noting the diversity of interpretations of this term, resulting from its global reach and multifaceted meaning in various contexts. This approach allows for the consideration of both universal and specific features of threats, which is crucial for a fuller understanding of them and effective countermeasures. The term 'to threaten' can be defined in accordance with P. Bączek's

[1] J. Grubicka, *Współczesny człowiek wobec zagrożeń w cyberprzestrzeni – studium z zakresu bezpieczeństwa personalnego*, Wydawnictwo Naukowe Uniwersytetu Pomorskiego w Słupsku, Słupsk 2025, p. 28.

proposal, who presents the lexical meaning of this concept as threatening someone, foretelling something bad, a warning under the threat of specific consequences and also as a situation in which something or someone becomes dangerous to another person or object.[2] From a political science perspective, P. Bączek defines threats as challenges that have not been addressed in time or at all. S. Koziej, on the other hand, describes a threat as a destructive impact on a subject, which may be indirect or direct. He divides these threats into potential and real, subjective and objective, external and internal, as well as military and non-military. In a non-military context, he places information threats alongside political, economic, social and environmental threats.[3] Such a classification points to a wide range of phenomena that may constitute a threat in various spheres of human activity. It is worth noting that not every phenomenon capable of affecting security can be unambiguously defined as a threat. This is because a state of threat is linked to the subjective awareness of the individual who is a potential target of a given phenomenon. This means that a lack of adequate knowledge about the nature and essence of a given phenomenon can lead to the perception of a threat as a specific mental state. Consequently, a better understanding and proper recognition of the nature of the threat allows for a reduction in the sense of danger. In such cases, a more appropriate term for the situation that has arisen is 'risk',[4] which can be controlled, or a 'challenge' that must be addressed, or a challenge worth taking on.[5] Identifying the sources of threat allows us to distinguish between internal information security threats, arising within the organisation, such as the threat of data loss, damage or service disruption due to error or accident, the risk of loss or damage through deliberate actions by dishonest users, as well as external threats arising outside the organisation as a result of deliberate or accidental actions by third parties. With regard to the system, experts also distinguish physical threats, in which damage is caused by an accident, failure or other unforeseen event affecting the information system.[6]

Against this background, the research problem addressed in the article concerns the relationship between the changing spectrum of cyber threats and the level and nature of risk to the personal security of individuals operating in cyberspace. The

[2] P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek, Toruń 2006, p. 31.

[3] S. Koziej, *Teoria sztuki wojennej*, Bellona, Warszawa 2011, p. 269.

[4] Risk is the uncertainty associated with one's own actions and their consequences; it is the danger of undesirable consequences of one's own actions. See S. Koziej, *Teoria…*, op. cit., p. 280.

[5] M. Wrzosek., *Polska, Unia Europejska, NATO wobec wyzwań i zagrożeń*, AON, Warszawa 2012, p.14.

[6] A. Żebrowski, W. Kwiatkowski, *Bezpieczeństwo informacji III Rzeczypospolitej*, Oficyna Wydawnicza ABRYS, Kraków 2000, p. 65.

problem is expressed in the following research question: How and to what extent do contemporary cyber threats determine risk to personal security in cyberspace, and which mechanisms of risk analysis and risk management are of key importance for limiting their consequences?

The main aim of the study is to identify and systematise the principal categories and sources of cyber threats affecting personal security, to clarify the relationship between cyber threat and risk, and to determine the significance of risk analysis, risk assessment and risk-management mechanisms for the protection of individuals in the digital environment.

The research hypothesis assumes that contemporary cyber threats constitute a significant determinant of risk to personal security in cyberspace and that the effective reduction of this risk requires systematic identification and assessment of threats combined with an interdisciplinary set of technical, organisational, legal and educational measures.

To address the research problem and assess the hypothesis, the study adopts a qualitative theoretical and analytical approach. The research methods include critical analysis of the literature in security studies, cybersecurity and risk management; analysis of normative and standardisation documents, including PN-I-13335-1:1999, ISO/IEC 27005:2022 and NIST SP 800-30 Rev. 1; comparative analysis of selected approaches to risk identification and assessment; and synthesis and classification used to organise threat categories, risk components and protective measures. The article is based on desk research and does not report empirical survey or experimental results.

Classification and sources of information security threats

Information security is threatened by a variety of factors which may be either accidental or deliberate in nature. The literature on the subject identifies many potential sources of threats that affect organisations, users and infrastructure. An analysis of the works of authors such as K. Liderman,[7] P. Bączek[8] and A. Żebrowski[9] allows these threats to be systematised and divided into various categories, taking into account both technological aspects and human actions. K. Liderman highlights a wide range of threat sources, including forces of nature, human error, deliberate

[7] K. Liderman, *Bezpieczeństwo informacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2012, p. 23.
[8] P. Bączek, *Zagrożenia informacyjne…*, *o*p. cit., pp. 74–76.
[9] A. Żebrowski, W. Kwiatkowski, *Bezpieczeństwo informacji…*, op. cit., p. 65.

malicious acts, hardware and software failures, as well as problems with service infrastructure.[10] P. Bączek classifies threats as random, traditional information-related, technological and civil rights-related,[11] whilst emphasising that their source may be human or organisational activity. R. J. Sutton[12] and A. Żebrowski[13] expand on this perspective by identifying specific techniques used by perpetrators, such as cyberattacks, exploiting system vulnerabilities or deliberate manipulation of information. In the context of information system security, a threat refers to potential events or actions that may lead to a breach of data integrity, confidentiality or availability, and consequently cause loss, damage or other adverse effects on the system, the organisation or its users. According to the PN-I-13335-1:1999 standard,[14] a threat is defined as a potential cause of an undesirable incident, the result of which may be damage to the resources of an information system, an institution or individuals. Although the concept of a threat seems intuitive, the process of identifying them is complex due to the diversity and variability of potential risk factors. Threats may be external in nature – such as cyberattacks, natural disasters or infrastructure failures – or internal, resulting, for example, from human error, deliberate malicious acts or organisational procedural shortcomings. The dynamic development of technology and the growing dependence of organisations and individuals on digital systems further complicate threat analysis. A modern approach to IT security therefore requires continuous monitoring, adaptation and integration of technology, procedures and user education in order to minimise potential risks.

The volatility and diversity of threats in cyberspace require a dynamic and flexible approach to their identification, classification and management. This poses challenges for both cybersecurity experts and organisations responsible for protecting IT systems. One of the key aspects in this context is data management, which plays an increasingly strategic role in the era of growing digitalisation. A world full of networked devices, such as mobile devices, sensors, applications and websites,

[10] See further K. Liderman, *Bezpieczeństwo informacyjne…*, op. cit., p. 23.

[11] P. Bączek, *Zagrożenia informacyjne…*, op. cit., p. 75.

[12] R.J. Sutton, *Bezpieczeństwo telekomunikacji*, Wydawnictwa Komunikacji i Łączności, Warszawa 2004, p. 17.

[13] A. Żebrowski, W. Kwiatkowski, *Bezpieczeństwo informacji…*, op. cit., p. 65.

[14] PN-I-13335-1:1999 is a Polish standard entitled *Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele bezpieczeństwa systemów informatycznych* ["Information technology – Guidelines for the management of information system security. Concepts and models of information system security"]. This standard is the equivalent of the international technical report ISO/IEC TR 13335-1, also known as GMITS (*Guidelines for the Management of IT Security)*. This document provides guidelines on the management of information technology security, discussing terminology, relationships between concepts and basic models.

generates vast amounts of information. It is estimated that over 2.5 trillion bytes of data are generated every day, and 90% of all data in the world has been created in the last two years.[15] The proliferation of technologies such as social networks, IoT devices and multimedia applications is contributing to this rapid growth. However, the greatest challenge is not the storage of this data itself, but its effective processing and analysis in order to draw useful conclusions. The management of the collected, processed and shared information is of key importance, as it allows not only for increased operational efficiency but also for the minimisation of risks associated with data security within the digital ecosystem.

Risk as a category of security assessment in cyberspace

System security is influenced by many factors, including threats, system vulnerabilities, risk and the value of the protected assets. Threats arise not only from obvious weaknesses, but also from their exploitation by attackers, which can lead to incidents compromising the integrity, confidentiality or availability of the system. Vulnerabilities are defined as weaknesses in a resource or group of resources that can be exploited by a threat. Together with the probability of their occurrence (risk) and the value of the resources, they form a risk management model. An integral part of management is recognising the existence of risk, assessing it and managing it – that is, acknowledging its severity and determining how to mitigate or eliminate it. Research by the SANS Institute[16] has identified the greatest risks associated with the Internet of Things, which include: problems with updating device software, the use of devices as the least secure points of entry into the network for subsequent infections or attacks, DoS (*Denial of Service)*, which in the case of, for example, energy network infrastructure or medical devices can lead to serious consequences; unauthorised modifications to device operating parameters; user errors and accidental modifications, which in networks of highly interconnected systems can lead to consequences that are difficult to predict across the entire system of connected devices.[17]

---

[15] Ł. Kryśkiewicz, *Wyzwania IoT w biznesie – potencjalne zagrożenia i niedogodności*, Dziennik Internautów, http://di.com.pl/wyzwania-iot-w-biznesie-potencjalne-zagrozenia-i-niedogodnosci-56027, (accessed 21.12.2025); J. Pescatore, *Securing the Internet of Things Survey*, SANS Institute InfoSec Reading Room, http://www.sans.org/reading-room/whitepapers/covert/securing-internet-things survey-34785, (accessed 5.12.2024).

[16] J. Pescatore, *Securing…*, op. cit.

[17] J. Grubicka, *Analiza zagrożeń ekosystemu IoT/IoE szacowania ryzyka bezpieczeństwa informacji*, "Rocznik Bezpieczeństwa Morskiego" 2022, vol. XVI, p. 509.

In natural language, risk denotes a measure or assessment of a threat or danger arising either from probable events beyond our control or from the possible consequences of a decision. In the broadest sense, risk is an indicator of a state or event that may lead to losses. It is proportional to the probability of that event occurring and to the magnitude of the losses it may cause.

The concept of risk, as the possibility of a specific undesirable outcome occurring at a certain time and under specific circumstances, is represented by a simple mathematical formula, a combination of two components: the probability of a threat causing undesirable outcomes and the magnitude of the outcomes resulting from the threat:[18]

$$R = P + S$$

where: R – risk,

P – probability of occurrence,

S – consequence (magnitude of loss or damage).

In classical mathematical decision theory, risk concerns a situation in which selecting a given decision option entails the possibility of various negative and positive consequences occurring, with the probability of each possibility being known. Formally, decisions made under conditions of risk refer to a class of decision-making problems in which, for every possible decision, the probability distribution of all its consequences is known.[19] Contemporary technical culture and the tradition of engineering awareness allow for a broader view of the continuity of technical systems' operation. The influence of the natural environment, the technical environment and the social environment on the continuity of various systems,[20] including safety management systems, is taken into account. It is worth noting that risk is a multidimensional phenomenon. If the potential impact of an event is significant and the probability of its occurrence is high, ignoring such a risk can lead to serious consequences.[21] When assessing risk, one must take into account both the severity of the potential consequences of a given event and the actual probability of its occurrence. For example, in a situation where there is a high risk of an attack on a company's IT systems and the consequences could be catastrophic, it becomes essential to implement appropriate preventive measures immediately. Conversely, events with a very low probability of occurrence but potentially significant impact also need

[18] K.R. Zieliński, *Ochrona ludności. Zarządzanie kryzysowe*, Difin, Warszawa 2017, p. 70.

[19] T. Kaczmarek, *Ryzyko i zarządzanie ryzykiem. Ujęcie interdyscyplinarne*, Difin, Warszawa 2005.

[20] J.R. Rak, M. Kwietniewski, *Bezpieczeństwo i zagrożenia systemów zbiorowego zaopatrzenia w wodę*, Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2011, pp. 23–28.

[21] Ł. Olejnik, A. Kurasiński, *Filozofia cyberbezpieczeństwa. Jak zmienia się świat? Od złośliwego oprogramowania do cyberwojny*, Wydawnictwo Naukowe PWN, Warszawa 2022, p. 30.

to be included in the risk analysis and should not be completely overlooked. The risk assessment process is complex and requires the consideration of many variables. It is not limited to simple mathematical calculations, but requires the use of dedicated tools and analytical methods that take into account the specific nature of the environment in question and the nature of potential threats. Effective risk management requires continuous monitoring and the adaptation of measures to changing conditions and the evolution of hazards.[22]

Currently, risk is defined as a four-element set:[23]

$$R = (S_i, P_{Si}, C_{Si}, O_{Si})$$

where: S_i – the i-th emergency scenario,

P_{Si} – the probability of the i-th emergency scenario occurring,

C_{Si} – the magnitude of losses caused by the realisation of the i-th emergency scenario,

O_{Si} – protection against the i-th emergency scenario.

Major civilisational and environmental disasters have sparked interest in risk within the fields of engineering and environmental protection. Risk assessment is now recognised as the basis for implementing effective preventive measures to enhance safety levels. In particular, the need to minimise the likelihood of a threat to life or health is widely accepted.[24]

The results of the risk assessment form the basis for taking corrective and preventive actions of a risk management nature. The protective measures are as follows:

- technical, reducing the hazard at source,
- organisational and legal,
- organisational and individual.[25]

The level of acceptable risk for the risk acceptance scenario is introduced and comprises four categories of risk acceptance criteria:

- acceptable risk (A) – no additional safety measures are required; current solutions and the resources allocated to them are accepted; and monitoring measures;

[22] See further D.W. Hubbard, R. Seiersen, *Metody modelowania, pomiaru i szacowania ryzyka*, Helion, Gliwice 2024, pp. 30–34.

[23] J. Rak, B. Tchórzewska-Cieślak, *Metoda analizy i oceny ryzyka w systemie zaopatrzenia w wodę*, Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2005, pp. 45–52.

[24] R. Wolniak, B. Skotnicka, *Metody i narzędzia zarządzania jakością. Teoria i praktyka*, Wydawnictwo Politechniki Śląskiej, Gliwice 2007.

[25] See further J. Grubicka, *Selected determinants of threats resulting from the implementation of the IoT/IoE concept*, "De Securitate et Defensione. O Bezpieczeństwie i Obronności" 2023, vol. 8, no. 2, pp. 97–98.

- tolerated (permissible) (T) – an assessment of alternatives should be carried out to determine whether the introduction of minor organisational, legal or functional changes would contribute to improving security or the perception of it;
- conditionally tolerated risk (WT) – additional security measures should be introduced within 6 months; the solutions in use should be improved;
- unacceptable risk (N) – immediate action must be taken to enhance security; additional/new measures must be introduced.

Risk management, and thus the implementation of security policy, cannot take place without the participation of those who wish to feel safe, and indeed have an inalienable right to such participation. On the other hand, those whose duty it is to ensure security must, by virtue of their responsibilities, make specific decisions. Decisions concerning the community, related to risk management, should be limited only by human rights and freedoms.[26] Public sensitivity to civil rights and freedoms, linked in this case to the unforced, voluntary acceptance of a level of risk and explicit consent to it, is in many cases the crux of the matter. The fundamental principle of voluntary risk acceptance underlies risk management and constitutes one of its most essential elements. Risks associated with the forces of nature are more acceptable (lightning strikes, severe storms, snowstorms) than risks imposed by human activity (cyberattacks, explosions, radiation associated with nuclear energy). Tolerance for each type of risk varies depending on its perception.[27]

Risk is a measure characterising safety (safety level) or the perception thereof, expressed as the probability of an adverse event occurring within a specified time, together with its consequences that negatively affect human health and life, property or the environment.[28]

The above definition highlights the existence of two aspects of risk assessment: the probability of an event occurring within a specified time and the consequences of that event. Risk analysis is based on examining the interrelationship between the probability and consequences of an event occurring. It is very rarely possible to quantify both values simultaneously, and thus with a high degree of precision. However, in many cases, even a rough estimate of these figures is sufficiently accurate to form the basis for making appropriate decisions and adopting measures to mitigate risk. Risk reduction therefore involves reducing probability. Risk analysis involves classifying individual risks, taking into account probability, consequences and lead time.

[26] R. Wolniak, B. Skotnicka, *Metody i narzędzia zarządzania jakością. Teoria i praktyka*, Wydawnictwo Politechniki Śląskiej, Gliwice 2007.
[27] J. Wolanin, *Zarys teorii bezpieczeństwa obywateli*, DANMAR, Warszawa 2005, p. 64.
[28] J. Grubicka, *Selected determinants…*, op. cit., pp. 97–98.

The probability of an event associated with a specific hazard can be divided into five classes, depending on the estimated frequency of its occurrence. The use of a risk matrix enables the determination of the risk level and the identification of how it is accepted. Accepted risk does not require the introduction of additional security measures as current solutions, resources and monitoring activities are considered sufficient. Tolerated risk requires an assessment of whether the introduction of organisational, legal or functional changes could contribute to improving security or the perception of it. Conditionally tolerated risk implies the need to implement additional safety measures and improve existing solutions within a specified time-frame. Unacceptable risk requires immediate action to enhance safety levels and the introduction of new or additional solutions. In engineering and the social sciences, risk is measured as the probability of an event, e.g. equipment failure, the destruction of a city by a hurricane, the outbreak of a flu epidemic or radioactive contamination, and as a measure of the damage caused by that event to society. In project management and profit-oriented companies, risk denotes a greater or lesser likelihood of unexpected circumstances occurring that have a negative impact on a project or the company's financial position. The probability of a harmful event occurring and the magnitude of potential losses are estimated using various methods and depend on numerous specific factors characterising a given situation, e.g. its frequency in the past. Unfortunately, a lack of full knowledge of these factors and the uncertainty of estimates mean that, as a result, many individual or group decisions depend on a subjective perception of risk, which in turn can lead to catastrophic human errors. Risk assessment is directly linked to a person's mental and physical state, as well as to the information, knowledge and preferences they possess – that is, what they have learnt, what they are capable of doing and what is important to them. Risk perception (not the risk itself) also depends, amongst other things, on trust in the source of information and the expected benefits.

Identifying an unacceptable risk requires a decision, but this decision may lead to further losses that also involve our preferences and emotions. Therefore, when acting, we often overestimate or underestimate risk. From this perspective, every person tries to minimise their own risk and maximise benefits, provided such action does not conflict with their ethical principles and is not influenced by their emotional state. Risk that arises during the course of action requires countermeasures, but this, in turn, may entail, for example, the loss of expected profits or the failure of the undertaking and the loss of invested or committed funds. It then becomes necessary to clarify priorities so as not to end up in a situation where the action taken is aimed at achieving conflicting goals, or one in which, by ignoring the identified

unacceptable risk, we stubbornly continue to act. This boils down to the fact that, because a new (unforeseen) risk has arisen, the decision-making process should be repeated.

Cyber threats and personal security

In an era of widespread digitalisation, where technology permeates almost every aspect of life, personal security in cyberspace is becoming one of the key challenges of our time. Cyber threats, such as the loss of personal data, identity theft, financial crime or disruptions to digital systems can have far-reaching consequences for both individuals and communities. In the face of these challenges, threat analysis and risk assessment related to personal security in the digital environment are essential for effective protection against potential incidents. The first step in the threat analysis process is to identify potential sources of risk that may threaten an individual's security in cyberspace.

Table 1 presents the key sources of risk affecting personal security in cyberspace, which form the basis for understanding contemporary challenges in this area and developing effective countermeasures.

Table 1. Key sources of risk affecting personal security in cyberspace

Threat category	Threat description	Examples
Identity theft	Gaining access to personal data in order to impersonate the victim.	Theft of login credentials, fake social media profiles, taking out loans using someone else's details.
Phishing	Attempts to obtain confidential information through fake messages or websites.	Emails impersonating banks, text messages with fake links, messages claiming to offer prizes.
Cyberbullying	Psychological abuse online, including offensive comments, threats or public humiliation.	Trolling, spreading false information, harassment on social media.
Ransomware	Malware that blocks access to data and demands a ransom to unlock it.	Encryption of files on the user's computer, demanding payment in cryptocurrency for the decryption key.

Threat category	Threat description	Examples
Social engineering attacks	Psychological manipulation aimed at gaining access to information or resources.	Impersonating IT staff, phishing for passwords over the phone, fake requests for technical support.
Malware	Software designed to spy, destroy data or steal information.	Viruses, keyloggers, spyware, applications installed without the user's consent.
Privacy breach	Unauthorised disclosure or use of a user's personal data.	Monitoring of online activity, location tracking, sale of data by apps.
Disinformation	The dissemination of false information to manipulate public opinion or individual behaviour.	Fake news, disinformation campaigns, manipulated photos or videos.
Technology addiction	Excessive use of digital devices leading to a negative impact on mental and physical health.	Compulsive scrolling through social media, addiction to online gaming, doomscrolling.
Cyberstalking	Persistent tracking or harassment of users online.	Monitoring social media activity, sending unsolicited messages, online threats.

Source: own compilation.

In the age of widespread digitalisation, where almost every aspect of life is linked to technology, personal safety in cyberspace has become one of the key challenges for individuals and communities. Cyber threats can have serious consequences, ranging from the loss of personal data, through identity theft, to financial crime. Consequently, threat analysis and risk assessment for personal security in cyberspace are essential processes for ensuring adequate protection. The first step in threat analysis is to identify potential sources of risk that may affect personal security in cyberspace. Table 2 illustrates the key stages of threat analysis and risk management in cyberspace, presenting a systematic approach to identifying, assessing and minimising risk. Each stage describes specific actions aimed at protecting individuals from threats and enhancing the effectiveness of personal security management in the digital environment. *Risk assessment* is one of the most important steps in this process, as it enables the estimation of the likelihood of threats occurring and their potential impact on the individual. In this context, probability analysis is of key importance, as it allows the frequency of threats such as phishing or malware attacks to be determined. Impact assessment, in turn, focuses on examining the potential

consequences of threats, including financial, legal and social implications. The results of this analysis allow risks to be classified as low, medium or high, which facilitates the prioritisation of security measures. Once the risk has been assessed, risk management strategies are implemented, such as risk avoidance, mitigation, transfer or acceptance. For example, risk avoidance involves refraining from actions that pose a threat, such as opening suspicious links, whilst mitigation involves the use of security technologies, such as two-factor authentication (2FA) or software updates. In certain cases, where the risk is low, it is also possible to accept it or transfer it to other parties, e.g. by taking out appropriate insurance. The dynamic nature of cyberspace requires the monitoring and review of the strategies employed, which includes regular security audits, system updates and user education. Of particular importance here is the role of education and awareness, which are key to building users' competence in responding to threats. Educational initiatives, such as training and awareness campaigns, can significantly reduce the risk of users falling victim to cybercrime.

Table 2. Key stages of threat analysis and risk management in cyberspace

Stage	Description	Examples and actions
Threat identification	Identifying potential sources of risk that may affect personal security in cyberspace.	• Phishing: the extraction of confidential information. • Malware: malicious software. • DDoS attacks, identity theft.
Risk assessment	Estimating the likelihood of threats occurring and their potential impact on the individual.	• Probability analysis: determining the frequency of threats. • Impact assessment: financial, legal and social consequences.
Risk management strategies	Implementation of measures aimed at reducing, eliminating or transferring risk.	• Risk avoidance: avoiding clicking on unknown links. • Risk reduction: software updates, 2FA.
Monitoring and review	Regular tracking of new threats and assessment of the effectiveness of protective measures	• Regular security audits, system updates, user education.
Education and awareness	Raising users' awareness of threats and how to respond to them.	• Educational campaigns, training, access to information resources.

Source: own work based on D.W. Hubbard, R. Seiersen, *Metody modelowania, pomiaru i szacowania ryzyka*, Helion, Gliwice 2024, pp. 30–34.

Table 2 is not only a summary of key risk management activities and stages, but also a tool facilitating the implementation of a comprehensive approach to personal

protection in a rapidly evolving digital environment. The processes and strategies outlined aim to enhance individual security whilst minimising potential losses resulting from cyber threats. Assessing the security of modern individuals in cyberspace requires the application of advanced methods of risk analysis and assessment, which take into account rapidly evolving threats and the growing complexity of technology.[29] Contemporary approaches to risk management focus on identifying potential threats, assessing their likelihood and determining the consequences for individuals and organisations. Both classical risk analysis methods and modern theoretical models adapted to the specific nature of the digital environment are of key importance here.

Risk analysis and assessment in the context of cybersecurity is a key element of effective threat management in the digital environment. There are many methods and tools available for identifying potential sources of risk, classifying them and developing strategies to minimise the negative impacts of threats. Classic methods, such as qualitative and quantitative risk analysis, form the basis of effective assessment. Qualitative analysis allows for a subjective assessment of risks, based on expert experience, whilst quantitative analysis enables a precise estimation of the probability and consequences of threats based on numerical data.[30] Methods such as SWOT[31] help to identify the strengths and weaknesses of the security system, as well as the opportunities and threats in the environment. This approach facilitates the planning of risk management strategies in the face of cyber threats. In more advanced cases, tools such as OCTAVE and FMEA (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*) are used. OCTAVE, as a structured approach, focuses on identifying key assets, potential threats and system vulnerabilities, enabling the creation of tailored risk management plans. In contrast, FMEA (*Failure Mode and Effects Analysis*) analyses potential failures and their consequences, which is particularly important in IoT and OT environments, where technological failures can lead to serious losses. In the context of global risk management standards, ISO/IEC 27005[32] and NIST SP 800-30[33] offer detailed guidelines on the identification, analysis and management of risk. The NIST SP 800-30 document describes a detailed risk assessment

[29] J. Grubicka, *Selected determinants…*, op. cit., pp. 97–98.

[30] S. Biedugnis, M. Smolarkiewicz, P. Podwójci, A. Czapczyk, *Ciągłość działania rozległych układów technicznych*, "Rocznik Ochrona Środowiska" 2009, vol. 11.

[31] J. Grubicka, *Selected determinants…*, op. cit., p. 97.

[32] D.W. Hubbard, R. Seiersen, *Metody modelowania…*, op. cit., pp. 30–34.

[33] SWOT – a popular heuristic technique used to organise and analyse information. The name is an acronym of the English words describing the four components of the analysis (*Strengths, Weaknesses, Opportunities* and *Threats)*. See further https://snl.no/SWOT-analyse, (accessed 28.12.2025).

process, covering: the identification of threats and vulnerabilities, the estimation of the likelihood of threats occurring, the analysis of potential consequences and the impact of threats on the organisation, and the development of recommendations for risk management. These standards provide a comprehensive approach to the protection of information systems and data. Modern models, such as Zero Trust and CIAS,[34] address the challenges of contemporary technologies. The Zero Trust model eliminates default trust in users and devices, enforcing continuous identity verification and the minimisation of privileges. The CIAS model, in turn, extends the classic CIA triad (Confidentiality, Integrity, Availability) to include a safety component, which allows for the assessment of risks associated with technological failures and manipulation. In practice, these methods are applied in various scenarios, such as:

- Protection against phishing and ransomware attacks through the analysis of threat patterns and the implementation of security measures.
- Risk assessment of IoT technology implementation, particularly in smart homes, to protect privacy.
- Implementation of the Zero Trust model in remote working environments to protect organisational systems.
- Development of a strategy for the protection of critical infrastructure, taking into account the risk of manipulation of OT technologies.[35]

The application of appropriate risk analysis and assessment methods enables more informed decision-making, reduces losses and enhances the security of both organisations and individuals in the digital environment. In the face of dynamic technological changes, it is crucial to combine traditional and modern approaches in order to address contemporary threats in a comprehensive and effective manner.

[34] ISO/IEC 27005:2022 *Information security, cybersecurity and privacy protection – Guidelines on information security risk management*, https://www.iso.org/standard/80585.html, (accessed 28.12.2025).

[35] NIST SP 800-30 is a document developed by the *National Institute of Standards and Technology* (NIST), which provides guidelines for risk assessment in the context of information security. The official title of this publication is: '*Guide for Conducting Risk Assessments'*, and its latest version is NIST *Special Publication 800-30 Revision 1*, published in September 2012. NIST SP 800-30 is widely used in organisations as a standard risk management tool, particularly in conjunction with other documents in the NIST series, such as NIST SP 800-39 ('*Managing Information Security Risk'*) or NIST SP 800-53 ('*Security and Privacy Controls for Information Systems and Organizations'*). The document is available on the official NIST website: https://csrc.nist.gov/publications/detail/sp/800-30/ rev-1/final, (accessed 28.12.2024). It is worth noting that the guidelines contained in NIST SP 800-30 are particularly useful for government institutions and private organisations seeking to standardise risk assessment processes as part of their information security strategies.

Conclusion

Cyber threats constitute a significant determinant of risk to the personal security of individuals operating in cyberspace. Their complex, variable and multidimensional nature means that they cannot be analysed solely in technical terms, but require an interdisciplinary approach combining the perspectives of security studies, computer science, law, psychology, sociology and education. The analysis conducted indicates that personal security in the digital environment depends on the proper identification of threat sources, the assessment of system and user vulnerabilities, and the estimation of the likelihood and consequences of potential incidents. Of particular significance are threats such as identity theft, phishing, cyberbullying, ransomware, social engineering attacks, malware, privacy breaches and disinformation. Their consequences may include financial losses, data loss, damage to reputation, a reduced sense of security, as well as negative psychological and social effects. A key conclusion is the need to treat risk analysis and assessment as a fundamental tool for managing security in cyberspace. Identifying threats, determining their likelihood, assessing possible consequences and selecting appropriate protective measures help to mitigate the negative consequences of cyber incidents. It is equally important to establish a risk acceptance level, as not every risk can be completely eliminated, but it can be managed consciously.

Effective protection of personal security in cyberspace therefore requires systematic monitoring of threats, the implementation of technical, organisational and legal solutions, as well as the development of users' digital literacy. Education is of particular importance as it raises awareness of threats and strengthens an individual's ability to make safe decisions in the digital environment. In this context, cybersecurity becomes not only the task of institutions and organisations, but also an element of the individual responsibility of every user of cyberspace. Taken together, the findings support the research hypothesis formulated in the Introduction: cyber threats are a significant determinant of personal-security risk, while effective risk reduction requires systematic assessment and the integration of technical, organisational, legal and educational measures.

Bibliography

Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek, Toruń 2006.

Biedugnis S., Smolarkiewicz M., Podwójci P., Czapczyk A., *Ciągłość działania rozległych układów technicznych*, "Rocznik Ochrona Środowiska" 2009, vol. 11.

Grubicka J., *Analiza zagrożeń ekosystemu IoT/IoE szacowania ryzyka bezpieczeństwa informacji*, "Rocznik Bezpieczeństwa Morskiego" 2022, vol. XVI.

Grubicka J., *Selected determinants of threats resulting from the implementation of the IoT/IoE concept*, "De Securitate et Defensione. O Bezpieczeństwie i Obronności" 2023, vol. 8, no. 2.

Grubicka J., *Współczesny człowiek wobec zagrożeń w cyberprzestrzeni – studium z zakresu bezpieczeństwa personalnego*, Wydawnictwo Naukowe Uniwersytetu Pomorskiego w Słupsku, Słupsk 2025.

Hubbard D.W., Seiersen R., *Metody modelowania, pomiaru i szacowania ryzyka*, Helion, Gliwice 2024.

Kaczmarek T., *Ryzyko i zarządzanie ryzykiem. Ujęcie interdyscyplinarne*, Difin, Warszawa 2005.

Koziej S., *Teoria sztuki wojennej*, Bellona, Warszawa 2011.

Liderman K., *Bezpieczeństwo informacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2012.

Olejnik Ł., Kurasiński A., *Filozofia cyberbezpieczeństwa*, *Jak zmienia się świat? Od złośliwego oprogramowania do cyberwojny*, Wydawnictwo Naukowe PWN, Warszawa 2022.

PN-I-13335-1:1999, *Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele bezpieczeństwa systemów informatycznych*, Polski Komitet Normalizacyjny, Warszawa 1999.

Rak J., Kwietniewski M., *Bezpieczeństwo i zagrożenia systemów zbiorowego zaopatrzenia w wodę*, Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2011.

Rak J., Tchórzewska-Cieślak B., *Metoda analizy i oceny ryzyka w systemie zaopatrzenia w wodę*, Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2005.

Sutton R.J., *Bezpieczeństwo telekomunikacji*, Wydawnictwa Komunikacji i Łączności, Warszawa 2004.

Wolanin J., *Zarys teorii bezpieczeństwa obywateli*, DANMAR, Warszawa 2005.

Wolniak R., Skotnicka B., *Metody i narzędzia zarządzania jakością. Teoria i praktyka*, Wydawnictwo Politechniki Śląskiej, Gliwice 2007.

Wrzosek M., *Polska, Unia Europejska, NATO wobec wyzwań i zagrożeń*, AON, Warszawa 2012.

Zieliński K.R., *Ochrona ludności. Zarządzanie kryzysowe*, Difin, Warszawa 2017.

Żebrowski A., Kwiatkowski W., *Bezpieczeństwo informacji III Rzeczypospolitej*, Oficyna Wydawnicza ABRYS, Kraków 2000.

ISO/IEC 27005:2022, *Information security, cybersecurity and privacy protection – Guidance on managing information security risks*, https://www.iso.org/standard/80585.html, (accessed 28.12.2025).

Kryśkiewicz Ł., *Wyzwania IoT w biznesie – potencjalne zagrożenia i niedogodności*, Dziennik Internautów, http://di.com.pl/wyzwania-iot-w-biznesie-potencjalne-zagrozenia-i-niedogodnosci-56027, (accessed 21.12.2025).

NIST SP 800-30 Rev. 1, *Guide for Conducting Risk Assessments*, https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final, (accessed 28.12.2025).
Pescatore J., *Securing the Internet of Things Survey*, SANS Institute InfoSec Reading Room, http://www.sans.org/reading-room/whitepapers/covert/securing-internet-things survey-34785, (accessed 5.12.2025).
SWOT-analyse, https://snl.no/SWOT-analyse, (accessed 28.12.2025).

Summary

The aim of the article was to identify and systematise the principal categories and sources of cyber threats affecting the personal security of modern individuals, to clarify the relationship between cyber threat and risk, and to determine the significance of risk analysis, risk assessment and risk-management mechanisms for protecting individuals in the digital environment. The research problem focused on how contemporary cyber threats determine the level and nature of personal-security risk in cyberspace and which mechanisms are most relevant to limiting their consequences.

The study used a qualitative theoretical and analytical approach. The research methods comprised critical analysis of the literature in security studies, cybersecurity and risk management; analysis of normative and standardisation documents, including PN-I-13335-1:1999, ISO/IEC 27005:2022 and NIST SP 800-30 Rev. 1; comparative analysis of selected approaches to risk identification and assessment; and synthesis and classification. Particular attention was given to identity theft, phishing, cyberbullying, ransomware, social engineering, malware, privacy breaches and disinformation, as well as to the role of risk identification, assessment and treatment.

The analysis supports the research hypothesis that contemporary cyber threats constitute a significant determinant of risk to personal security in cyberspace and that effective risk reduction requires systematic threat identification and assessment combined with technical, organisational, legal and educational measures. The conclusions emphasise continuous monitoring, conscious risk acceptance, appropriate protective strategies and the development of users' digital awareness as essential components of personal security in the digital environment.