ASEJ ISSN: 2543-9103 ISSN: 2543-411X (online)

The current state of research in the area of identification and analysis of threats resulting from cybercrime

Zbigniew Małodobry[1], Laura Misztal[2], Sebastian Piotrowski[3]

1 University of Rzeszów
Poland

2 Military University of Technology
Poland

3 Bielsko-Biala University of Applied Sciences
Poland

***Abstract*— This article examines the current state of research on cybercrime, focusing on its key actors, targets, and methods of counteraction. It highlights the growing scale, complexity, and economic significance of cyber threats, as well as the increasing role of artificial intelligence in both offensive and defensive activities. The study also identifies major research gaps and emphasizes the need for integrated and interdisciplinary approaches to effectively address cybercrime.**

Keywords— cybercrime, cybersecurity, artificial intelligence, cyber threats, digital security

I. INTRODUCTION

The modern information society operates in an environment of intense digitization, encompassing virtually all spheres of social, economic, and political life. The development of digital technologies, including the Internet of Things (IoT), artificial intelligence (AI), and cloud services, generates new opportunities, but also leads to the emergence of new categories of threats. One of the most significant problems is cybercrime, whose scale and complexity are growing exponentially. Cybercrime encompasses a wide spectrum of activities, from relatively simple online frauds to highly sophisticated operations conducted by organized crime groups or state actors. This phenomenon is cross-border in nature, which further complicates its effective combating (D. S. Wall, 2007, pp. 1–15). Recent years have seen a significant increase in the number of studies on cybercrime, conducted by both academic communities and state institutions and international organizations. These studies are interdisciplinary in nature and encompass technical, legal, economic, and social approaches.

The purpose of this article is to identify key research centers, define the main research areas, analyze existing research results, and identify research gaps and directions for further research.

II. CYBERCRIME RESEARCH CENTERS

In Poland, research on cybercrime is conducted by a variety of entities, including research institutes, technical universities, and interdisciplinary centers. NASK, the National Research Institute, plays a key role, implementing advanced projects in threat detection, malware analysis, and the use of artificial intelligence to identify dangerous content (NASK, 2023, pp. 5–20).

Technical universities, such as the AGH University of Science and Technology, Warsaw University of Technology, and Wrocław University of Science and Technology, also play a significant role, developing research on information system security, cryptography, and critical infrastructure protection. Humanities and social science centers, including the University of Silesia, focus on analyzing the social and political aspects of

ASEJ - Scientific Journal of Bielsko-Biala School of Finance and Law
Volume 30, No 2 (2026), pages 5
https://doi.org/10.19192/wsfip.sj2.2022.11
Received: January 2026 Accepted: April 2026
Published: June 2026

cybercrime, including perpetrator motivations and the impact of cyberthreats on society.

Cardinal Stefan Wyszyński University (KRSW) is active in countering cybercrime through research on cyberthreats and cybersecurity issues. Another important area of its activity is educating highly qualified personnel for work in the data protection and information systems security sectors. Furthermore, the university collaborates with public institutions and other entities, supporting the development of legal solutions and practices for preventing and combating cybercrime.

Internationally, research on cybercrime is conducted at the most renowned academic institutions. Among the most important are Carnegie Mellon University, particularly through the CERT Coordination Center, specializing in incident analysis and risk modeling (CERT Coordination Center, 2022, pp. 3–12); Massachusetts Institute of Technology and Stanford University, focusing on cryptography and systems security; the University of Oxford, developing research in cybersecurity policy; Royal Holloway, University of London, one of the pioneering centers for information security research; Simon Fraser University, conducting criminological research on cybercrime as part of the International CyberCrime Research Centre; and the Cambridge Cybercrime Centre, one of the most influential academic centers in the world. His specialty is the analysis of massive cybercrime datasets. He builds some of the largest cybercrime databases and makes data available to researchers globally. This center is often considered the most "scientifically advanced" (data-driven). UCD Centre for Cybersecurity & Cybercrime Investigation - Considered a leader in Europe. It collaborates closely with Interpol and Europol. It trains services from over 40 countries and combines research with investigative and operational practice. Center for Cybercrime Studies - One of the main centers in the US. It has an interdisciplinary approach (law, criminology, and IT). It analyzes topics such as the darknet, drug trafficking, and financial crime. This center is a leader in the criminological understanding of cybercriminals. Cybercrime Research Institute - A think tank collaborating with the UN, governments, and large companies. It develops global strategies and policies. It has a strong influence on cybersecurity law and policy worldwide.

III. Research units of state services

A key component of the research system are units operating within state agencies (e.g., incident response teams – CERTs, CSIRTs). Their activities are operational and analytical in nature and include threat monitoring, incident analysis, and the development of cybercrime countermeasures. State agency research units play a key role in the cybercrime countermeasures system, providing analytical, technological, and expert support for authorities responsible for national security. Within the Police, the Central Bureau for Combating Cybercrime (CBZC) plays a particularly important role, carrying out both operational and analytical tasks, conducting research on new forms of cybercrime, identifying trends, and developing methods to combat them. This activity includes malware analysis, monitoring online threats, and developing tools to support the detection and prosecution of perpetrators.

The Internal Security Agency (ABW), responsible for protecting the country's internal security, including countering strategic threats in cyberspace, also plays a significant role in cybersecurity research. Within its remit, the Internal Security Agency conducts advanced threat analysis, develops cyberintelligence capabilities, and collaborates with other national and international institutions to exchange information and best practices.

Research units and structures subordinate to the Ministry of National Defense also play a significant role in the system, including the Cyberspace Defense Force, which is responsible for developing the country's defense capabilities in cyberspace. Their activities include research on modern information technologies and the development of tools for protecting critical infrastructure and military systems. This system is complemented by the Military Communications Institute, which conducts research and development in communications, cryptography, and IT security, thus supporting the development of innovative cybersecurity solutions.

The cooperation of these entities enables the creation of a coherent system for responding to cyber threats, based on the integration of scientific research, operational activities, and technological development. This enables not only the effective detection and combating of cybercrime but also the forecasting of future threats and the development of a long-term national security strategy.

IV. Cybercrime actors

Research on cybercrime actors focuses on identifying typologies of perpetrators, analyzing their motivations, and reconstructing their strategies. A multidimensional approach has emerged in the literature, taking into account technical, social, and economic factors. Three basic categories of perpetrators are distinguished: individuals acting individually, organized criminal groups, and state-sponsored entities (APTs – Advanced Persistent Threats). Research indicates that contemporary cybercrime increasingly takes the form of organized, quasi-business activities, with specialized roles such as malware creators, infrastructure operators, and financial intermediaries (T. J. Holt, 2016, pp. 45–70).

An important area of research is the analysis of the tools used by perpetrators. This particularly concerns advanced malware, botnets, attack automation tools, and the use of artificial intelligence to optimize criminal activities. Research into the economics of cybercrime is also gaining increasing importance, indicating that cybercriminals operate based on market mechanisms, utilizing the "cybercrime-as-a-service" (CaaS) model, enabling the rental of criminal tools and services (R. Leukfeldt, T. J. Holt, 2020, pp. 80–105).

Simultaneously, research into social engineering techniques, which constitute one of the most effective attack vectors, is developing. Analyses show that the use of psychological manipulation significantly increases the effectiveness of cybercriminal activities, especially in the context of phishing

and spear-phishing (C. Hadnagy, 2018, pp. 25–50).

V. CYBERCRIME SUBJECTS

The second key area of research is the identification of cybercrime targets, understood as goods, resources, and areas of social activity targeted by attacks. Research indicates that cybercrime encompasses a broad spectrum of targets, including personal and sensitive data, financial resources, critical infrastructure (e.g., energy, transportation, healthcare systems), intellectual property, and enterprise IT systems. The literature emphasizes the growing importance of attacks on critical infrastructure, which can lead to serious social and economic consequences, even threats to national security (P. W. Singer, A. Friedman, 2014, pp. 120–150).

Another important research direction is the analysis of the vulnerabilities of various social groups. It indicates that children and adolescents are particularly vulnerable to cyberbullying and abuse, the elderly are more likely to fall victim to financial fraud, and businesses are a prime target for ransomware attacks. Empirical research shows that the level of vulnerability to cyber threats is strongly correlated with the level of digital competences and awareness of users (S. Furnell, 2017, pp. 60–85).

VI. TECHNOLOGIES AND METHODS FOR COUNTERING CYBER THREATS

Contemporary research on countering cyber threats focuses not only on incident identification but primarily on building multi-layered digital resilience systems that integrate anomaly detection, behavior analysis, and automated response mechanisms. Moving away from classical signature methods toward approaches based on behavioral analysis and machine learning is one of the most important development directions in this field (R. Liu, J. Shi, X. Chen, C. Lu, 2024, pp. 10–35).

Intrusion detection systems (IDS/IPS) play a significant role, which in recent research are developed using deep learning methods and hybrid models. The literature emphasizes that combining various analytical techniques, such as ensemble classifiers, sequential models, and feature extraction algorithms, allows for more effective detection of both known and previously unknown threats (I. M. Sayem et al., 2024, pp. 1–10). At the same time, it is pointed out that the effectiveness of these systems in laboratory conditions does not always translate into their effectiveness in real-world environments, which is due, among other things, to data dynamics and imbalances (R. Sommer, V. Paxson, 2010, pp. 305–316).

Behavioral analysis, which enables the identification of incidents based on deviations from normal user and system activity patterns, is gaining increasing importance. This approach is particularly useful in detecting internal attacks and advanced APT campaigns, which are characterized by long-term persistence and high levels of stealth (A. Behl et al., 2023, pp. 140–170). In the context of emerging threats, particular attention is being paid to the use of artificial intelligence in detecting zero-day attacks. Models based on anomaly analysis, autoencoders, or representation learning enable the identification of potentially dangerous activities without the need to first define their signature (A. L. Buczak, E. Guven, 2016, pp. 1–20). At the same time, the development of these technologies brings new challenges, such as limited model interpretability and the risk of manipulation of their behavior.

This problem is reflected in research on adversarial machine learning, which indicates that AI-based systems can become targets for specialized attacks, including the manipulation of training data or the generation of adversarial examples (A. Vassilev et al., 2025, pp. 1–25). Consequently, the modern approach to cybersecurity requires the simultaneous protection of both the IT infrastructure and the analytical models themselves.

The importance of these issues is also confirmed by analyses of the current threat landscape, which indicate the continued dominance of ransomware attacks, data breaches, and incidents affecting service availability. This indicates the need to further develop solutions integrating detection, response and organizational resilience (ENISA, 2024, pp. 10–40).

VII. LEGAL AND REGULATORY ASPECTS

Research on cybercrime clearly indicates that the effectiveness of countering threats depends not only on technical tools but also on the quality and consistency of legal regulations. Cybercrime is cross-border in nature, which means that classic state jurisdiction mechanisms prove insufficient without extensive international cooperation (D. S. Wall, 2007, pp. 50–65). The fundamental regulatory instrument on an international scale remains the Council of Europe Convention on Cybercrime (Budapest Convention), which established common standards for the criminalization of computer-related crimes and procedures for securing electronic evidence. Its importance also lies in creating a framework for international cooperation enabling more effective prosecution of crimes in the digital sphere (Council of Europe, 2001/2024, pp. 1–30). In response to technological developments, additional protocols have been adopted to expand access to digital evidence in cross-border cases.

At the European Union level, the NIS 2 Directive, which introduces a comprehensive approach to cybersecurity risk management, is of key importance. This regulation expands the scope of entities covered by the obligations, introduces more stringent incident reporting requirements, and strengthens management's responsibility for the security of IT systems (European Union, 2022, pp. 1–50). Considering risks in supply chains is particularly important, reflecting the evolving nature of modern threats.

Another important element of the regulatory development is the Cyber Resilience Act, which establishes cybersecurity requirements for products with digital elements. This regulation is based on the principles of "security by design" and "security by default," imposing on manufacturers the obligation to ensure

security during the design and distribution of products. This shifts responsibility from end users to technology producers.

These actions are complemented by initiatives strengthening cooperation at the EU level, such as the Cyber Solidarity Act, which aims to develop joint incident response capabilities and improve information exchange between member states (Council of the European Union, 2024, pp. 5–15). The introduction of such mechanisms demonstrates the growing importance of a collective approach to cybersecurity management. At the same time, regulatory developments are creating significant tensions between security and the protection of individual rights, particularly in the areas of privacy and personal data protection. The literature emphasizes the need to maintain a balance between the effectiveness of security measures and respect for fundamental rights, which is one of the key challenges facing contemporary cybersecurity legislation.

VIII. THE MOST IMPORTANT RESEARCH RESULTS

Research into cybercrime to date has yielded a number of significant results, including: the development of threat detection methods – advanced intrusion detection systems (IDS) and machine learning-based systems have been developed, enabling the identification of previously unknown threats; cyber risk modeling – models have been developed to assess the level of risk in IT systems and predict potential incidents; economic analysis of cybercrime – research has shown that cybercrime is one of the most profitable areas of criminal activity globally (Europol, 2023, pp. 25–60); the development of legal regulations – new legal regulations regarding data protection and cybersecurity have been introduced in many countries (e.g., GDPR); and increased public awareness – educational campaigns and training programs have contributed to increased awareness of threats.

It is difficult to pinpoint a single "most important" research result, as this field combines technology, psychology, and economics. However, the discovery of the economic structure of cybercrime-as-a-service (Cybercrime-as-a-Service) is considered a breakthrough. The most significant research in this area was conducted by scientists from the University of California, San Diego (UCSD) and Berkeley (USA) in 2011. Here's why this result is crucial:

1. Understanding the "bottleneck": Researchers penetrated spam operations and discovered that while hackers can easily change servers or domains, their weakest point is the payment system. It turned out that just a few banks worldwide handled 95% of transactions related to the illegal trade in pharmaceuticals via spam.
2. Shifting strategy: Thanks to this discovery, law enforcement agencies stopped focusing solely on prosecuting code authors and began targeting the financial chain (follow the money), which proved to be a much more effective method of combating mass cybercrime.
3. Specialization: This research proved that cybercrime is not about individual hackers, but a specialized market, where one entity provides email databases, another creates viruses, and yet another launders the money. Here are the most interesting and important findings from the latest cybercrime research (2024–2026)—a structured overview of trends that are truly changing the landscape of this phenomenon:

Cybercrime has reached the scale of a "global economy" (losses in 2024: approximately $9.5 trillion annually, comparable to the world's 3rd largest economy; new academic research suggests a more conservative, but still significant, figure of ~$500 billion annually). Conclusion: Cybercrime is no longer an "IT problem"—it is now one of the largest global economic phenomena.

Avalanche-like increase in the number of attacks (+28% attacks quarterly (2024), Record 1,300+ attacks per week per organization, in Poland: +23% incidents year-on-year). Conclusion: Not only is the scale growing—attacks are becoming a daily reality for organizations. Artificial intelligence is changing the rules of the game (AI can already win hacking competitions (CTFs) against humans, automating vulnerability searches, phishing, and malware creation). Conclusion: We are entering an era where cybercrime can be cheaper, faster, and automated, and the barrier of entry for criminals is drastically lowered.

Attacks are becoming increasingly sophisticated and "intelligent." Research indicates the development of advanced threat techniques (TTPs), and the increased use of social engineering, deepfakes, and targeted attacks (APTs). Conclusion: Cybercrime is shifting from "mass attacks" to precise psychological and technical operations.

Most companies are still victims of attacks – 75% of companies have experienced a cyber incident within a year. Consequences: reputational damage, decreased customer trust, operational downtime. Conclusion: A cyberattack is no longer a question of "if," but rather "when and how severe." The most groundbreaking research findings: Economic scale larger than most countries, Steady, rapid increase in the number of attacks, automation of cyberattacks by AI, increasingly precise and psychological methods, commonality of incidents in companies, connections with state activity and geopolitics.

IX. RESEARCH GAPS AND DIRECTIONS FOR FURTHER RESEARCH

Despite the rapid development of research, significant gaps remain. The most important include an insufficient understanding of the mechanisms of operation of organized cybercrime groups, the limited effectiveness of methods for detecting new, unknown threats (so-called zero-day threats), the lack of coherent models for international cooperation, and insufficient consideration of social and psychological aspects.

Future research should focus on integrating technical and social approaches, utilizing artificial intelligence in threat analysis, developing methods for predicting cyberattacks, and strengthening international cooperation.

X. CYBERCRIME SUBJECTS

Cybercrime today targets diverse areas of human activity that have become digitized and operate in the information space. This particularly applies to areas related to professional life, where ICT systems are used for data processing, communication, and organizational process management. Cybercrime in this area includes, among other things, unauthorized access to information, theft of sensitive data, and disruption of IT infrastructure. An equally significant area of cybercrime's impact is an individual's personal life, including interpersonal communication and activity in digital media, where privacy violations, identity theft, and cyberbullying can occur.

Another important area is the household, which, with the development of smart technologies (the so-called Internet of Things), is becoming vulnerable to external interference, leading to compromised user security. Cybercrime also affects property and savings, particularly in the context of electronic banking and online financial services, where phenomena such as phishing, malware, and financial fraud occur. Entertainment and education are also areas of concern, where threats include, among others, cybercrime. Illegal content distribution, copyright infringement, and information manipulation. Cybercrime also impacts various social groups, which, due to their demographic characteristics and levels of digital literacy, demonstrate varying levels of vulnerability to threats. Particular attention is paid to children and adolescents, who, as heavy users of digital technologies, are vulnerable to phenomena such as cyberbullying, grooming, and internet addiction. Seniors, on the other hand, often characterized by lower levels of digital literacy, constitute a group particularly susceptible to online fraud, manipulation, and data theft. Therefore, countering cybercrime requires considering the specifics of individual areas of social life and adapting preventive and educational activities to the needs of specific social groups.

XI. REFERENCES

Wall D. S., (2007) Cybercrime: The transformation of crime in the information age, Cambridge.

NASK – Państwowy Instytut Badawczy, (2023) Raport o stanie cyberbezpieczeństwa w Polsce, Warszawa.

CERT Coordination Center, (2022) Annual Threat Report, Pittsburgh.

Holt T. J., (2016) Cybercrime through an interdisciplinary lens, New York.

Leukfeldt R., Holt T. J., (2020) The human factor of cybercrime, New York.

Hadnagy C., (2018) Social engineering: The science of human hacking, Indianapolis.

Singer P. W., Friedman A., (2014) Cybersecurity and cyberwar: What everyone needs to know, Oxford.

Furnell S., (2017) Cybersecurity in the digital age, London.

Liu R., Shi J., Chen X., Lu C., (2024) Network anomaly detection and security defense technology based on machine learning: A review, London.

Sayem I. M., et al., (2024) ENIDS: A deep learning-based ensemble framework for network intrusion detection [w:] „IEEE Transactions on Network and Service Management", no. 21(5), New York.

Sommer R., Paxson V., (2010) Outside the closed world: On using machine learning for network intrusion detection [w:] „IEEE Symposium on Security and Privacy", Berkeley.

Behl A., et al., (2023) Cybersecurity analytics: A stochastic model for insider threat detection, Cham.

Buczak A. L., Guven E., (2016) A survey of data mining and machine learning methods for cyber security intrusion detection [w:] „IEEE Access", New York.

Vassilev A., et al., (2025) Adversarial machine learning: A taxonomy and terminology of attacks and mitigations, Gaithersburg.

ENISA, (2024) ENISA Threat Landscape 2024, Athens.

Council of Europe, (2001/2024) Convention on Cybercrime, Strasbourg.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 (NIS 2), (2022) Bruksela.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2847 (Cyber Resilience Act), (2024) Bruksela.

Council of the European Union, (2024) Cybersecurity package, Brussels.

Europol, (2023) Internet Organised Crime Threat Assessment (IOCTA), Haga.