The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

Cybersecurity and Law

2025 Nr 1(13)

DOI: 10.35467/cal/214597

Crisis situation in cyberspace – the ICT dimension of critical infrastructure security

Bartłomiej TEREBIŃSKI
Akademia Sztuki Wojennej
ORCID: 0000-0002-6124-9905
E-mail: b.terebinski@akademia.mil.pl

Abstract

The aim of this article is to describe how to achieve cybersecurity in the area of national security and international organizations, particularly crisis management related to critical IT infrastructure, information crisis management, and building resilience to cyber threats. In an increasingly interconnected digital world, cybercrises have become a serious threat to organizations, governments, and society at large. These crises, encompassing a spectrum of malicious activities such as data breaches, ransomware attacks, and system failures, can have catastrophic consequences beyond immediate financial losses. The ubiquity of cyberthreats not only threatens individual organizations but also poses a significant risk to national security, economic stability, and public trust. Understanding the multifaceted nature of cybercrises and developing effective management strategies are essential to mitigating their effects and protecting our digital infrastructure.

In an increasingly digital world, cybersecurity has become a key element of organizational resilience and integrity. Technological advances have led to the increasing complexity and frequency of cyberthreats, necessitating a structured and strategic approach to managing such crises. The cybersecurity crisis management process is typically divided into distinct phases, each with specific goals and actions aimed at limiting damage and restoring normalcy. Understanding these phases: identification, containment, and elimination, is essential for organizations seeking to minimize the impact of cybersecurity incidents.

Effective cybersecurity crisis management is a multifaceted process that begins with the rapid identification of incident indicators and then rapid containment to prevent further damage. Once an incident is contained, organizations must rigorously eliminate malicious elements and patch exploited vulnerabilities to restore system integrity. The next phase of recovery involves restoring operations, monitoring residual threats, and

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

verifying system security, ensuring a safe return to normal. Post-incident analysis provides crucial information about the attack, enabling necessary policy adjustments and strengthening defenses. Throughout the entire process, transparent communication and collaboration with external entities, as well as adherence to legal standards, are crucial to maintaining stakeholder trust and accountability. Finally, a commitment to continuous improvement (through policy revisions, technology investments, and ongoing staff training) ensures organizations are resilient to future cyber threats. Ultimately, these phases create a comprehensive framework that not only addresses current crises but also strengthens long-term cybersecurity resilience, protecting organizational assets and reputation in an increasingly digital environment.

Keywords

critical infrastructure, cyber crisis situations, early detection systems, heuristic analysis

Introduction

In general, a crisis situation encompasses the factors, stages, and events preceding and shaping a crisis. Crisis situations are defined as a state of increasing instability, uncertainty, and social tension, posing a threat to territorial integrity, life, health, property, cultural heritage, the environment, or critical infrastructure. However, a crisis should be distinguished from situations such as: a catastrophe, a situation that destroys existence and leaves no chance of survival; disruptions that cause a temporary loss of financial liquidity but can be resolved using one's own resources; and conflicts arising from hidden and acute contradictions between personnel, leading to difficulties in managing the organization. Every crisis, regardless of its origins, is, on the one hand, a complex phenomenon, and this complexity takes the form of a complex structure. On the other hand, it follows a similar course, which facilitates its structural and functional identification. Crisis identification is a necessary condition for formulating a crisis problem, i.e., defining the scope of actions necessary to overcome it. The phases of the crisis cycle include: crisis symptoms, escalation ending in a crisis, and de-escalation, which ends the crisis when a new level of stability is reached.

A state when the curve is within the limits of standard events is called normal. The harbingers of an emerging threat are the symptoms (signs, manifestations, signs) of this threat, which, if left unaddressed, escalate the situation. This causes it to exceed the acceptable level of stability, which can sometimes exceed the capabilities of a standard response. At this level, standard procedures are usually sufficient, and it is not necessary to take remedial steps using additional procedures to manage the situation. Responding to the development of a normal situation involves monitoring the threat landscape, which in turn allows for the discovery and explanation of emerging symptoms and the prediction of developments ultimately preventing the exceedance of applicable standards. These standards are pre-defined and reflect the human environment in terms of physical, biological, and sociocultural dimensions. If the situation changes in such

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

a way that the accepted standards are exceeded, it indicates the development of a crisis. The stage of threat escalation occurs, i.e., the development of a crisis situation, which involves decision-making outside of normal procedures. It is necessary to combat the threat and implement rescue and technical actions. It should be emphasized here that the availability of current information on the threat status and trends, as well as actual time reserves, are always critical factors in developing and selecting the final decision. In the crisis de-escalation phase, the most crucial factors are the development and organization of a process for combating the threat's effects and providing assistance to those in need. Therefore, personnel, information, and technical and material support will be crucial here.

The aforementioned classification of crisis situations is based on the occurrence of several characteristics, occurring separately or in combination. Therefore, the characteristics of a crisis are:

- the presence of a critical event located on a so-called continuum of events, extending from values perceived as minimum to values perceived as maximum,
- the perception of a critical event as unexpected, threatening the loss of valuable values, creating a sense of threat and uncertainty about the future,
- loss of control over ongoing events, as existing ways of behaving become unhelpful and necessitate changes in existing ways of functioning, both individually and collectively[1].

In terms of the characteristics of crisis situations, the literature groups them as follows:

- Group I – related to humans and their physiological and psychological problems.
- Group II – concerns human communities and refers to anything that threatens the loss of life and health, national and ethnic identity (related to violations of human rights) this includes nationalism, chauvinism, cultural and religious discrimination, and racism – all of which give rise to social crises.
- Group III – covers events related to ecology and environmental protection (concerns human living conditions) these are situations related to both human activity and natural factors – which can generally lead to an ecological crisis.
- Group IV – covers issues of production, exchange of goods, rational management, i.e., low rates of economic development, disparities in economic development in a given region (among other countries).
- Group V – concerns threats to state security on a national and supranational level.

[1] Zob.: J. Ziarko, J. Walas-Trębacz, Podstawy zarządzania kryzysowego. Część. 1 Zarządzanie kryzysowe w administracji publicznej, Kraków 2010.

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

Crises can be classified using various criteria. Therefore, the following factors will be relevant to the classification: the ability to adapt to changes caused by the crisis, the process-based nature of crisis management within the organization, the phase of the organization's life cycle, the time between the first symptoms of a problem and the crisis situation's occurrence (the so-called warning period), the location of the problem, the triggers of the crisis, and the sphere of the organization affected by the crisis. Each of these areas can be related to cyberspace operations, particularly its ICT dimension.

Critical infrastructure and cyber crisis situations

Critical infrastructure comprises systems and resources whose failure or destruction could lead to serious consequences for public safety, health, the economy, or the functioning of the state[2]. This infrastructure includes, among others, energy, transportation, telecommunications, water supply, and information systems. Cyberattacks on critical infrastructure can take various forms, from ransomware to DDoS attacks, which can paralyze systems. The increasing number of threats, such as attacks by state actors, hacker groups, and terrorists, necessitates the continuous monitoring and updating of security systems. Information and communication technologies play a key role in ensuring the security of critical infrastructure. Monitoring systems, data analysis, encryption, and blockchain technology can increase resilience to attacks. Integrating new technologies, such as artificial intelligence, enables faster threat detection and response.

In crisis situations, contingency plans and response procedures are crucial. Regular exercises and attack simulations can help prepare teams to respond effectively to an incident. Collaboration with government institutions, the private sector, and international organizations is essential for exchanging information and best practices. Raising awareness among employees and users of IT systems about cybersecurity threats is crucial. Training and information campaigns can significantly reduce the risk of human error, which is often the weakest link in a security system. Many countries are implementing regulations regarding critical infrastructure protection. Standards such as NIST[3], ISO/IEC 27001[4], and EU regulations such as the GDPR[5] aim to ensure an adequate level of security and data protection. Crisis management in cyberspace is a complex process that requires the cooperation of many entities and continuous adaptation to changing conditions and threats. In an increasingly interconnected world, cyberspace has become the backbone of modern society, supporting the operation and security of

[2] https://www.gov.pl/web/rcb/infrastruktura-krytyczna [access:10.11.2025].
[3] https://www.nist.gov/ [access:10.11.2025].
[4] https://www.isms.online/iso-27001/#:~:text=ISO/IEC%2027001%20to%20norma%20dotycz%C4%85ca%20zarz%C4%85dzania%20bezpiecze%C5%84stwem,ocen%C4%99%20ryzyka%2C%20zarz%C4%85dzanie%20ryzykiem%20i%20ci%C4%85g%C5%82e%20doskonalenie. [access: 10.11. 2025].
[5] https://uodo.gov.pl/404 [access:10.11.2025].

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

critical infrastructure sectors. With increasing dependence on digital systems, vulnerability to cybercrise (disruptive events that threaten the stability, security, and resilience of critical services) also increases. These crises can range from targeted cyberattacks to widespread data breaches and catastrophic system failures, often unfolding with alarming speed and scale.

Cybercrisis situations take many forms, each with different characteristics and implications for critical infrastructure. The most common are targeted cyberattacks, in which cybercriminals seek to exploit system vulnerabilities to cause disruption or gain unauthorized access. Another common form is data breaches, which involve the unauthorized extraction or disclosure of confidential information, undermining trust and operational integrity. System failures, often resulting from software vulnerabilities, hardware failures, or cyberattacks, can lead to the shutdown of critical services. For example, the 2015 cyberattack on the Ukrainian power grid, which left hundreds of thousands without power, demonstrates how a well-coordinated attack can quickly escalate into a large-scale crisis. Such incidents often escalate rapidly, with cybercrises spreading rapidly across networks, simultaneously affecting multiple sectors. The pervasive impact of these crises extends beyond immediate operational disruptions to include economic losses, threats to public safety, and national security. Recent cybercrises, such as ransomware attacks on healthcare systems during the COVID-19 pandemic and the compromise of satellite communications networks[6], highlight the evolving threat landscape and underscore the urgent need for resilient cybersecurity measures in critical infrastructure.

Critical infrastructure sectors operating in cyberspace encompass a complex set of interconnected systems essential to the functioning of society. Energy and utility systems underpin daily life, encompassing energy generation, transmission, and distribution networks. Disruptions in these areas can escalate into broader crises, as exemplified by the 2010 Stuxnet malware attack on Iranian nuclear facilities, which demonstrated how cyberweapons can sabotage physical infrastructure[7]. Transportation networks, including air traffic control, rail systems, and maritime navigation, rely heavily on digital systems for security and efficiency; disruptions in cyberspace can cause accidents, delays, and even fatalities. Communication networks, including internet providers, satellite systems, and emergency services, are essential for the coordination and dissemination of information, and their disruption can isolate populations or hinder crisis response. Financial and healthcare systems are equally critical; cyber incidents affecting banking infrastructure can disrupt economic transactions, and breaches of healthcare databases threaten patient safety and confidentiality. The interconnectedness of these sectors amplifies the potential consequences of cyber crises, underscoring the importance of integrated security frameworks that protect their digital interdependencies.

[6] https://econjournals.sgh.waw.pl/KNoP/article/download/4754/4799/11570 [access:10.11.2025].
[7] J. Jānis, Was stuxnet an act of war?, „Security Forum” 2017, vol. 1 no. 1, pp. 109-121.

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

Understanding the cyber threat landscape requires recognizing the diverse actors with diverse goals posing a threat to critical infrastructure. State-sponsored cyber actors operate based on strategic objectives, often linked to national security interests, espionage, or geopolitical influence. For example, nation-states have been implicated in advanced operations targeting energy or government networks, as exemplified by alleged Russian cyber activities against Western infrastructure. Hackers and terrorist groups, driven by ideological motives or seeking to create chaos, have also targeted critical systems; notable examples include attacks on financial institutions or communication networks to disseminate political messages or destabilize societies. Insider threats, targeting employees or contractors with privileged access, pose a unique challenge due to their intimate knowledge of systems and the potential for sabotage or inadvertent errors[8]. Criminal organizations, motivated by profit, are increasingly exploiting cybersecurity vulnerabilities through ransomware, phishing, and data theft, often operating across borders for financial gain. The convergence of these threat actors creates a complex threat environment that requires comprehensive, multi-layered cybersecurity strategies, international cooperation, and proactive intelligence sharing to effectively mitigate risk[9].

One of the fundamental challenges in protecting critical infrastructure from cyberattacks is the inherent technological vulnerabilities that permeate digital systems. Many industries still operate with outdated hardware and legacy software that lack necessary security patches and are not resistant to modern cyberthreats. These outdated systems often provide entry points for cybercriminals, who can relatively easily exploit known vulnerabilities. Furthermore, organizations often implement insufficient cybersecurity protocols, resulting in gaps in their security. These vulnerabilities can include weak password policies, inadequate access controls, or a lack of multi-factor authentication, increasing the likelihood of successful breaches. Moreover, the increasing interconnectivity of systems (while improving efficiency and operational coordination) significantly increases the attack surface. As various sectors and services become digital, a single point of failure or security breach can spread across multiple systems, amplifying the scope and impact of a cyber crisis. This interconnectivity creates a complex web of dependencies, making it difficult to contain breaches and quickly recover data. Such technological gaps underscore the urgent need for modernization, robust security frameworks, and continuous monitoring to strengthen resilience against evolving cyberthreats targeting critical infrastructure.

Sources of information about the crisis in cyberspace

[8] https://mobzilla.pl/najgrozniejsze-grupy-hakerskie-wspierane-przez-rzady-kto-naprawde-stoi-za-atakami [access: 10.11.2025].
[9] https://itwiz.pl/ransomware-phishing-i-generatywna-ai-w-krajobrazie-cyberbezpieczenstwa/ [access: 10.11.2025].

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

In an era where digital technology permeates every aspect of daily life, cybercrisis has become a matter of paramount importance for governments, corporations, and individuals. The pervasiveness of cyberthreats (from data breaches to advanced cyberattacks) requires a comprehensive understanding of the various information sources that shape our awareness and response strategies. These sources are multifaceted and include official government and cybersecurity agency reports, media and industry publications, as well as academic research and technical papers. Each plays a key role in shaping collective understanding of cyberthreats, their evolving tactics, and potential defenses. A detailed analysis of these sources reveals not only their individual contributions but also how they collectively contribute to a nuanced understanding of the ongoing cybercrisis.

Official reports from governments and cybersecurity agencies provide a foundation for reliable and structured information regarding cybercrisis[10]. These documents, such as national cybersecurity strategies and policies, define a country's overarching approach to preventing, detecting, and responding to cyberthreats. For example, the United States National Cyber Strategy outlines priorities for protecting critical infrastructure, fostering international cooperation, and promoting a resilient cyberdefense. Such strategic frameworks provide important reference points for decision-makers and cybersecurity professionals. Furthermore, incident reports and alerts issued by agencies such as the Computer Emergency Response Team (CERT)[11] or the Cybersecurity and Infrastructure Security Agency (CISA)[12] provide real-time information on current threats. These agencies monitor and analyze cyber incidents, distributing alerts that help organizations identify vulnerabilities and respond quickly. For example, CISA alerts on ransomware campaigns enable organizations to implement immediate countermeasures. Furthermore, these agencies collect and publish data and statistics on cyber threats and breaches, offering valuable insights into trends, attack vectors, and the scale of the crisis. This data-driven approach allows for policy adjustments and resource allocation, as seen in recent reports detailing the increase in supply chain attacks and the spread of phishing campaigns. Therefore, official reports and incident data are essential to providing a structured, reliable, and up-to-date perspective on the cyber threat landscape.

Media and industry publications are key channels for disseminating information about the cyber crisis to the public, industry stakeholders, and policymakers. News organizations consistently report on recent cyber incidents, often providing detailed descriptions of the attacks, their impact, and subsequent responses. For example, high-profile security breaches such as the SolarWinds

[10] https://www.gov.pl/web/cyfryzacja/krajobraz-cyberprzestrzeni-roczne-sprawozdanie-o-cyberbezpieczenstwie, https://cyberpolicy.nask.pl/aktualnosci/enisa-opublikowala-pierwszy-w-historii-raport-oceniajacy-stan-cyberbezpieczenstwa-w-unii-europejskiej/ [access: 11.10.2025].
[11] https://cert.pl/ [access:11.10.2025].
[12] https://www.cisa.gov/ [access:10.11.2025].

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

attack[13] and the Colonial Pipeline ransomware[14] incident received extensive media coverage, helping to raise public awareness and prompting regulatory action. In addition to ongoing reports, industry publications and cybersecurity journals offer in-depth analyses and expert opinion that contextualize these incidents within the context of broader trends. Articles in media outlets like Wired[15], The Hacker News[16], and cybersecurity journals like the Journal of Cybersecurity[17] often include technical analyses of attack methods such as zero-day exploits and supply chain vulnerabilities.

These analyses help explain complex cyberattack techniques to a wider audience, fostering understanding and vigilance. Furthermore, technology and cybersecurity companies regularly publish reports, white papers, and threat intelligence summaries that highlight emerging threats and innovative defense solutions. For example, reports from companies like FireEye[18] and CrowdStrike[19] provide insights into nation-state hacking campaigns and malware evolution, crucial for organizations seeking to adapt their defenses. Consequently, media and industry publications provide accessible, timely, and expert sources of information that inform diverse audiences about the constantly evolving cyberthreat landscape.

Research and technical studies provide a scientific foundation for understanding cybercrisis, offering robust analyses of threats and defenses based on empirical evidence and technical expertise. Researchers conduct extensive research on the evolving nature of cyberthreats, often employing advanced methodologies to track attack patterns and predict future trends. For example, academic studies have documented the rise of advanced persistent threats (APTs)[20] and their tactics, techniques, and procedures (TTPs), providing insight into how state-sponsored actors operate over extended periods to infiltrate vulnerable networks.

Technical analyses published in peer-reviewed scientific journals examine attack methods such as spear phishing, malware delivery, and zero-day exploitation, enabling cybersecurity professionals to understand the complexities of cyberattacks at a detailed level. These analyses also provide insights into the development of robust defense mechanisms, as research on cryptography, intrusion detection systems, and network segmentation advances the field's knowledge of best practices. White papers from leading cybersecurity companies and research institutions often synthesize this knowledge, offering strategic

[13] https://www.fortinet.com/resources/cyberglossary/solarwinds-cyber-attack [accessed: 10.11.2025].
[14] https://ieeexplore.ieee.org/document/10181159/ [access: 10.11.2025].
[15] https://www.wired.com/ [access: 11.11.2025].
[16] https://thehackernews.com/ [access: 11.11.2025].
[17] https://academic.oup.com/cybersecurity [access: 11.11.2025].
[18] https://fireeye.dev/docs/about/fireeye/ [access: 11.11.2025].
[19] https://www.crowdstrike.com/en-us/ [access: 11.11.2025].
[20] K. Singamaneni, S. Sukhvinder, A Comprehensive Survey on Advanced Persistent Threat (APT) Detection Techniques, „Computers, Materials & Continua" 2024, vol. 80 issue 2, pp. 1-10.

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

recommendations tailored to various sectors. For example, studies on the effectiveness of multi-factor authentication or zero-trust architectures provide practical guidance for organizations seeking to improve their security posture.

Overall, scientific research and studies deepen our theoretical and technical understanding of cyber threats, supporting evidence-based policymaking and innovative defensive strategies. Therefore, it can be concluded that the sources of information about the cyber crisis are diverse and interconnected, with each contributing in a unique way to understanding this complex problem. Official reports from governments and cybersecurity agencies provide reliable, strategic, and up-to-date data essential for informed policymaking and incident response. In the European Union, the main cybersecurity agency is ENISA (European Union Agency for Cybersecurity)[21], which supports member states, EU institutions, and businesses in developing and implementing cybersecurity strategies. In Poland, the Ministry of Digital Affairs (Chancellery of the Prime Minister) primarily coordinates activities in this area, managing the National Cybersecurity System (NCS) and acting as a single point of contact (SPC) for cybersecurity matters, enabling cooperation with other EU countries and responding to incidents (see: Table 1).

Furthermore, media and industry publications serve as accessible channels that translate technological developments into understandable narratives, increasing public awareness and industry preparedness. At the same time, scientific research and technical studies provide the theoretical and technical foundation necessary to develop cybersecurity practices and understand emerging threats. Together, these sources create a comprehensive knowledge ecosystem essential for addressing the ongoing cyber crisis. Recognizing the value and limitations of each source is crucial to developing a holistic and effective approach to cybersecurity, ensuring societal resilience in the face of the constantly evolving digital threat landscape.

Another area that must be emphasized in this discussion is understanding the motivations and perpetrators of cyber incidents targeting critical infrastructure. This is essential for developing effective defense strategies. State-sponsored actors pose some of the most sophisticated and persistent threats, often pursuing geopolitical objectives such as espionage, sabotage, or destabilization of adversary infrastructure. These actors, supported by national governments, employ advanced infiltration and disruption techniques, as exemplified by alleged cyber operations by Russia, China, and North Korea targeting power grids, government networks, and communications systems. In addition to state-sponsored threats, hackers and ideological groups pursue political or social goals, often launching cyberattacks to raise awareness, protest policies, or undermine authority. Their activities, while sometimes less technically sophisticated, can still cause significant disruption, especially when targeting systems of public importance. Insider threats pose a particular threat because employees or contractors with

[21] https://www.enisa.europa.eu/ [access: 11.11.2025].

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

privileged access can intentionally or unintentionally compromise systems (through malicious actions or negligence) leading to breaches or sabotage.

Table 1. *Cybersecurity Agencies in the EU and Poland*

Tasks	Purposes	Cooperation
European Union Agency for Cybersecurity (ENISA)		
ENISA provides support to Member States and EU institutions in key areas of cybersecurity, including the implementation of legislation such as the NIS Directive	It helps build trust in digital products and services by creating cybersecurity certification systems and supports countries in developing the information society.	The Agency works with EU countries and bodies to help them prepare for cybersecurity challenges.
Activities in Poland		
National Cybersecurity System (NCS)	A system managed by the Ministry of Digital Affairs (Chancellery of the Prime Minister) and which connects various entities responsible for protecting cyberspace.	
Ministerstwo Cyfryzacji (Chancellery of the Prime Minister)	It serves as the coordinator and single point of contact (SPoC) for cybersecurity in Poland.	
SPoC	Contact point in the Chancellery of the Prime Minister – responsible for receiving and forwarding reports of serious or significant incidents affecting at least two EU countries, and ensuring cooperation with other countries on cybersecurity issues.	

Source: *own study*.

Organized cybercriminal groups, primarily motivated by financial gain, are increasingly attacking critical infrastructure using advanced methods such as ransomware, data theft, and fraud. Their activities are often coordinated, cross-border, and highly lucrative, contributing to a complex threat landscape that requires multi-layered security measures, intelligence sharing, and international cooperation to effectively mitigate. Technological weaknesses constitute a fundamental vulnerability that cyber adversaries exploit to trigger crises in critical infrastructure. Many sectors still operate on legacy systems (outdated hardware and software) that lack necessary security updates or are incompatible with modern cybersecurity standards. These outdated systems provide easy entry points for attackers who can exploit known vulnerabilities to gain access to the system or cause it to fail. Furthermore, many organizations maintain inadequate security protocols, such as weak password policies, insufficient user authentication, and weak access controls, further increasing vulnerability to breaches. Patch management practices are often inconsistent or delayed, leaving systems vulnerable to threats that exploit known software vulnerabilities. The increasing

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

interconnectivity of critical systems, while increasing operational efficiency, simultaneously expands the attack surface, creating a web of dependencies that can spread vulnerabilities across sectors. For example, a breach of a connected supply chain or control system can result in cascading failures, making containment and recovery difficult. These technological weaknesses underscore the urgent need for modernization, comprehensive security protocols, and continuous vulnerability assessments to strengthen defenses against evolving cyberthreats.

Cybercriminals employ a wide range of techniques tailored to exploiting vulnerabilities in critical infrastructure systems. Phishing and social engineering tactics remain among the most common and effective methods, manipulating human psychology to trick employees into revealing confidential information or granting unauthorized access. Attackers create convincing emails or messages that appear authentic, leading to the theft of credentials or the installation of malware. Malware, ransomware, and viruses are used to infiltrate systems, disrupt their operation, or extort ransom from organizations by encrypting key data and demanding a ransom. Ransomware attacks have skyrocketed, crippling hospitals, power plants, and financial institutions by preventing access to critical data. Distributed Denial of Service (DDoS) attacks are another common method, overloading target networks with massive amounts of traffic, temporarily disabling services. Such attacks can be used as a smokescreen for more covert operations or as a way to destabilize services at critical moments. These techniques, often evolving in complexity, require advanced cybersecurity measures, threat intelligence, and proactive defense strategies to protect critical infrastructure assets from crippling disruptions and malicious exploitation. It's also worth mentioning sources of information about the cyber crisis in 2025 that may be helpful:

- European Commission – „Cybersecurity Blueprint” This is the European Union's official cyber crisis action plan, outlining the roles of institutions and procedures for responding to large-scale incidents. It was published on February 24, 2025;
- Council of the European Union – press release of June 6, 2025. Contains information on the adoption of an updated EU cyber crisis and incident management plan. This is an important document for understanding current strategies in this area.

In addition, it's worth following reports from organizations such as NATO, ENISA, and specialized industry publications, which regularly analyze the situation in cyberspace and provide information on the latest incidents and defense strategies.

Cyberspace early threat detection systems

Early cybersecurity threat detection systems are technologies and methods designed to identify potential attacks or security incidents before they occur

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

or at an early stage[22]. These systems continuously analyze network traffic for anomalies that may indicate attempted attacks, such as port scans or unusual communication patterns. They use advanced data analysis techniques, including machine learning, to predict and identify threats based on previous incidents and collected data. These systems are often integrated with threat databases that provide information on known attacks and techniques used by cybercriminals. They use rule sets and signatures to detect known threats, allowing for a rapid response to known attack techniques. If a threat is detected, these systems can automatically notify administrators of incidents, enabling rapid intervention. They work in conjunction with other security systems, such as firewalls and intrusion prevention systems (IPS), to provide comprehensive protection. They utilize behavioral analytics to detect unusual user behavior that may indicate internal threats or accounts being exploited by cybercriminals. Such systems are crucial in today's environment, given the growing number of cyber threats, and their effectiveness relies on continuous algorithm refinement and updated threat databases.

In a rapidly evolving cyberspace landscape, the proliferation of advanced cyber threats necessitates the development and implementation of robust early threat detection systems. These systems constitute the first line of defense, enabling organizations to identify and mitigate potential security breaches before they can cause significant damage. As cyber threats become more complex, the technologies and methodologies used to detect them must also evolve. Early threat detection systems encompass a variety of approaches, each tailored to detecting malicious activity through different mechanisms. Understanding the types of these systems, their core components, and the advanced technologies they rely on is crucial to appreciating their role in protecting digital assets and maintaining the integrity of the IT infrastructure.

Early threat detection systems are diverse and are primarily divided into signature-based, anomaly-based, and hybrid methods. Signature-based detection systems are among the earliest and simplest methods, relying on the identification of threats based on known patterns or malicious code signatures. For example, antivirus software often uses signature databases to detect known malware by comparing code signatures with a repository of malicious code signatures. While these systems are highly effective against known threats, they struggle to identify new or evolving attacks, limiting their scope in dynamic cyber environments. Anomaly-based detection systems, on the other hand, focus on identifying deviations from established, normal behavior within a network or system. These systems use statistical models or machine learning algorithms to flag unusual activity, such as incorrect login times or unexpected data transfers, which may indicate a security breach. A practical example is the use of anomaly detection in intrusion detection systems (IDSs), which monitor network traffic patterns

[22] https://www.grupae.pl/ids-vs-ips-roznice-i-zastosowanie-na-praktycznym-przykladzie/ [access: 11.11.2025].

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

to reveal subtle indicators of cyberattacks. Recognizing the limitations of both methods, hybrid detection systems have emerged, combining signature-based precision with anomaly-based adaptability. These integrated systems leverage the strengths of both approaches, enabling more comprehensive threat detection. For example, a hybrid system might use signature matching for known threats while simultaneously using anomaly detection to detect unknown or advanced attacks, thus providing a more resilient security posture.

The effectiveness of early threat detection systems depends on their core components, which include advanced data collection and monitoring tools, real-time analysis algorithms, and robust alerting and response mechanisms. Data collection tools continuously gather information from various sources, such as network traffic, system logs, and user activity, providing a comprehensive picture of the digital environment. For example, security information and event management (SIEM)[23] systems aggregate logs from servers, endpoints, and applications to facilitate centralized monitoring. Once the data is collected, real-time analysis algorithms immediately process it, identifying patterns or anomalies that may indicate malicious intent. Advanced algorithms leverage techniques such as statistical modeling, machine learning, and behavioral analytics to recognize subtle indicators of threats among massive volumes of data. An effective detection system must also incorporate rapid notification mechanisms that notify security teams of potential issues, enabling rapid investigation and mitigation. Response mechanisms, often automated, may include isolating compromised systems, blocking malicious IP addresses, or initiating predefined containment protocols. Integrating these components creates a dynamic and responsive security environment that can evolve with emerging threats, thereby minimizing potential damage and ensuring operational continuity.

The technological foundations of early threat detection systems are based on cutting-edge advances such as machine learning, artificial intelligence (AI), behavioral analysis, and pattern recognition techniques. Machine learning algorithms facilitate the identification of complex threat patterns that traditional rule-based systems might miss. For example, AI-based systems can learn from historical attack data to predict and recognize new forms of malware or intrusion techniques, significantly improving detection accuracy. Behavioral analysis techniques analyze user and system activity over time to establish baseline levels of normal behavior; deviations from these baselines trigger alerts. An example is the use of behavioral analytics to detect insider threats, where unusual access patterns or data exfiltration attempts are flagged for review. Pattern recognition and fingerprinting methods further enhance detection capabilities by comparing current activity with known malware signatures or creating unique identifiers (fingerprints) for suspected threats. These technologies often work synergistically, enabling detection systems to adapt and evolve in response to the constantly evolving tactics used by cybercriminals. Together, these technological foundations

[23] https://www.microsoft.com/en-us/security/business/security-101/what-is-siem [access: 11.11.2025].

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

provide a sophisticated arsenal that allows cybersecurity professionals to stay ahead of emerging threats and implement proactive defense strategies.

Early threat detection systems (ETS) deployment environments are as diverse as the threats they are designed to address, each offering unique advantages and challenges. One common environment is the network perimeter, where systems such as firewalls and intrusion detection systems (IDSs)[24] are integrated to monitor incoming and outgoing traffic. These perimeter defense systems provide the first line of defense, analyzing data packets and blocking suspicious activity before they penetrate deeper into the network. For example, firewalls configured with advanced threat detection capabilities can analyze traffic patterns and filter malicious requests, preventing threats from reaching internal systems. In addition to perimeter protection, endpoint- and device-based detection systems play a crucial role by directly monitoring individual devices such as laptops, servers, and mobile devices. These systems are essential for identifying threats that bypass network security or originate from infected endpoints, such as malware installations or unauthorized access attempts. With the growing popularity of remote work models in organizations, endpoint detection and response (EDR)[25] solutions have become crucial, providing real-time visibility into device-level threats. Furthermore, with the rise of cloud computing and hybrid infrastructures, organizations are deploying detection systems in cloud environments and hybrid configurations to provide comprehensive protection. Cloud-based detection tools can analyze massive amounts of data across distributed resources, leveraging a scalable infrastructure to detect threats in real time. These diverse deployment environments underscore the need for flexible and integrated detection strategies that can protect complex, multi-layered digital infrastructures.

Despite technological advancements, early threat detection systems face significant challenges that impact their effectiveness and reliability. A major problem is the prevalence of false positives, where benign activities are mistakenly flagged as malicious, leading to security personnel fatigue. This phenomenon can desensitize teams, causing them to miss or ignore real threats, thus undermining the overall security posture. The constantly evolving threat landscape further complicates detection efforts, especially with the emergence of zero-day vulnerabilities –vulnerabilities unknown to vendors or defenders at the time of their exploitation. Attackers exploit these unknown weaknesses to infiltrate systems undetected, rendering traditional signature-based methods insufficient and highlighting the need for adaptive, behavioral detection methods. Furthermore, the monitoring processes themselves raise concerns about privacy and data security. Collecting and analyzing massive amounts of sensitive information can inadvertently expose personal data or create additional attack vectors if not managed with strict security controls. These challenges require continuous refinement of

[24] https://www.fortinet.com/resources/cyberglossary/intrusion-detection-system [access: 11.11.2025].
[25] https://www.fortinet.com/resources/cyberglossary/what-is-edr [access: 11.11.2025].

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

detection methods, balancing sensitivity with accuracy, and implementing safeguards that protect user privacy while maintaining vigilance.

Recent technological advances have significantly enhanced the capabilities of early threat detection systems, enabling a more proactive and intelligent approach to security. One such advancement is the integration of big data analytics (Big Data), which allows systems to quickly process and analyze vast amounts of data from various sources. Big Data enables the identification of complex patterns and correlations that might escape traditional analysis, thus increasing the accuracy and speed of threat detection. Combined with this, predictive modeling uses machine learning algorithms to forecast potential threats based on historical data and emerging trends. This approach not only detects existing attacks but also predicts future ones, providing organizations with a strategic advantage in cybersecurity planning. Furthermore, the implementation of threat intelligence platforms has become a key element of modern detection systems. These platforms facilitate the real-time exchange of information on new threats, attack techniques, and indicators of compromise between organizations and the security community. Using shared intelligence, detection systems can quickly adapt to emerging threats, update signatures, and refine detection algorithms. Collectively, these advances foster a dynamic and resilient security environment capable of predicting and countering advanced cyber threats before they escalate into harmful incidents. The practical application of early threat detection systems has been powerfully demonstrated in various case studies, highlighting their effectiveness in real-world scenarios. One notable example is the detection of ransomware campaigns in corporate networks. Modern detection systems using behavioral analysis and anomaly detection have been able to identify unusual file encryption activity and suspicious communication patterns indicative of ransomware infiltration, often alerting security teams before widespread damage occurs. For example, some organizations have successfully thwarted ransomware attacks by deploying systems capable of recognizing the rapid file modifications typical of this type of malware, enabling proactive containment. Similarly, insider threats (where malicious or negligent employees compromise security) are increasingly being identified using advanced behavioral analytics.

By establishing baselines of typical user activity, detection systems can flag anomalies such as unauthorized data access or unusual login times, facilitating early intervention. Moreover, early warning capabilities for distributed denial of service (DDoS) attacks are crucial, especially during high-stakes events or on critical infrastructure. Detection systems monitor traffic flow and behavioral patterns across network nodes, enabling rapid identification of traffic spikes characteristic of DDoS attacks. This proactive detection allows organizations to quickly implement countermeasures, minimizing service disruptions.

These case studies highlight the crucial role integrated, advanced detection systems play in protecting digital assets from diverse and evolving cyberthreats. Looking ahead, the early threat detection landscape is poised for transformational advancements driven by technological innovation and strategic

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

change. A clear trend is the implementation of autonomous response systems that leverage artificial intelligence and machine learning not only to detect threats but also to initiate automated remediation without human intervention. This evolution aims to dramatically shorten response times, more effectively mitigate threats, and reduce the burden on security teams. Furthermore, there is a growing emphasis on expanding threat detection and proactive monitoring efforts. Instead of waiting for alerts, organizations are increasingly deploying dedicated teams and tools to actively search for hidden threats within their infrastructure, employing techniques such as threat intelligence analysis and hypothesis-driven investigations. This proactive approach increases the likelihood of detecting sophisticated attacks that evade traditional detection methods. Furthermore, the development of standardized frameworks for interoperability between different security tools and platforms is gaining momentum. Such standards facilitate seamless information sharing, integration of detection capabilities, and coordinated response across organizational units and technologies. This interoperability is crucial for building cohesive security ecosystems capable of countering complex, multi-dimensional cyberthreats in an increasingly connected digital world. These future trends promise to transform early threat detection from a reactive approach into an intelligent, predictive cybersecurity strategy.

In summary, early threat detection systems are fundamental to defending cyberspace against the ever-evolving array of cyberthreats (Table 2). A variety of detection methods, including signature-based, anomaly-based, and hybrid, provide organizations with comprehensive tools to effectively identify malicious activity. Their success relies on key components such as comprehensive data collection, real-time analysis, and rapid response mechanisms, supported by advanced technologies such as machine learning, behavioral analysis, and pattern recognition. Deployment environments spanning network perimeters, endpoints, and cloud infrastructures underscore the importance of flexible and integrated security strategies. Despite challenges such as false positives and evolving vulnerabilities, ongoing technological advances (such as big data analytics, predictive modeling, and threat intelligence sharing) are enhancing detection capabilities. Practical examples of ransomware mitigation, insider threat identification, and DDoS warning illustrate their practical value. Future trends toward autonomous response, proactive threat detection, and standardized frameworks promise to revolutionize cybersecurity, making early detection systems more proactive, intelligent, and resilient. Ultimately, these systems are crucial for maintaining the integrity and security of digital ecosystems in an increasingly interconnected world.

Table 2. *Early detection of cyber threats*

Types of early detection systems

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

Intrusion Detection Systems (IDS): These systems monitor network traffic and analyze it for suspicious activity. They can be host-based (monitoring individual devices) or network-based (monitoring traffic across the entire network).	Security Information and Event Management (SIEM): They integrate data from various sources (e.g., logs, security alerts) and analyze it in real time, allowing for the identification of threats and incidents.	Endpoint Detection and Response (EDR): They focus on monitoring and securing endpoints, such as computers and mobile devices, to detect and respond to threats early.
Detection technologies and methods		
Participating in networks: They use techniques such as Deep Packet Inspection (DPI), which analyze data transmitted over the network at the packet level.	Heuristic analysis: They use heuristic techniques that detect unknown threats by analyzing their behavior instead of relying on signatures.	Machine Learning and AI: Increasingly used in threat detection systems, they enable automatic learning from data and identifying patterns that may indicate danger.
Challenges and limitations		
False alarms: One of the main problems is false alarms, which can lead to wasted resources and decreased efficiency.	Threat Evolution: Cybercriminals are constantly changing their methods, requiring continuous updates and improvement of detection systems.	Infrastructure Complexity: As technology advances and IT environments become more complex, managing and integrating different early detection systems becomes increasingly difficult.

Source: *own study*.

Summary

In summary, critical infrastructure security in cyberspace faces a range of complex challenges stemming from the nature of cybercrisis situations, the interconnectedness of key sectors, and the diverse spectrum of malicious actors driven by geopolitical, ideological, or financial considerations. Rapidly escalating and widespread, cybercrises pose a significant threat to societal security, economic stability, and national security. Critical infrastructure components, including energy, transportation, communications, and healthcare systems, are increasingly vulnerable to technological vulnerabilities such as outdated equipment, insufficient security protocols, and a growing attack surface resulting from interconnectedness.

Perpetrators (from state-sponsored groups to organized cybercriminals) use advanced techniques such as phishing, malware deployment, and distributed denial-of-service (DDoS) attacks to achieve their destructive goals. Responding to these threats requires a comprehensive approach, encompassing resilient

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

technological defenses, continuous monitoring, effective response mechanisms, and international cooperation. As new technologies such as artificial intelligence and machine learning become integral to threat detection, and global standards develop, the future of cybercrisis management promises improved resilience. Ultimately, protecting critical infrastructure in cyberspace requires vigilance, innovation, and collaboration to ensure societal stability in the face of an evolving cyberthreat landscape.

Literature

Jānis J., Was stuxnet an act of war?, „Security Forum" 2017, vol. 1, no. 1.

Singamaneni K., Sukhvinder S., A Comprehensive Survey on Advanced Persistent Threat (APT) Detection Techniques, „Computers, Materials & Continua" 2024, vol. 80, no. 2.

Ziarko J., Walas-Trębacz J., Podstawy zarządzania kryzysowego. Część Zarządzanie kryzysowe w administracji publicznej, Kraków 2010.

https://academic.oup.com/cybersecurity.

https://cert.pl/.

https://www.enisa.europa.eu/.

https://www.crowdstrike.com/en-us/.

https://econjournals.sgh.waw.pl/KNoP/article/download/4754/4799/11570.

https://fireeye.dev/docs/about/fireeye/.

https://itwiz.pl/ransomware-phishing-i-generatywna-ai-w-krajobrazie-cyberbezpieczenstwa/.

https://www.microsoft.com/en-us/security/business/security-101/what-is-siem.

https://mobzilla.pl/najgrozniejsze-grupy-hakerskie-wspierane-przez-rzady-kto-naprawde-stoi-za-atakami.

https://thehackernews.com/.

https://uodo.gov.pl/404.

https://www.cisa.gov/.

https://www.fortinet.com/resources/cyberglossary/solarwinds-cyber-attack.

https://www.gov.pl/web/cyfryzacja/krajobraz-cyberprzestrzeni-roczne-sprawozdanie-o-cyberbezpieczenstwie, https://cyberpolicy.nask.pl/aktualnosci/enisa-opublikowala-pierwszy-w-historii-raport-oceniajacy-stan-cyberbezpieczenstwa-w-unii-europejskiej/.

https://www.gov.pl/web/rcb/infrastruktura-krytyczna.

https://ieeexplore.ieee.org/document/10181159/.

https://www.isms.online/iso-27001/#:~:text=ISO/IEC%2027001%20to%20norma%20dotycz%C4%85ca%20zarz%C4%85dzania%20bezpiecze%C5%84stwem,ocen%C4%99%20ryzyka%2C%20zarz%C4%85dzanie%20ryzykiem%20i%20ci%C4%85g%C5%82e%20doskonalenie.

https://www.nist.gov/.

https://www.wired.com/.