CYBER SECURITY OF CRITICAL INFRASTRUCTURE

Professional article

Ante Maksan, University of Applied Sciences in Security and Safety, Zagreb, Croatia, ante_maksan@yahoo.com

Luka Leško, University of Applied Sciences in Security and Safety, Zagreb, Croatia

“Abrstract”

Today, it is completely unimaginable to live without technology that permeates all areas of human activity - from communication, education and healthcare, to finance, transport and industry. Although ubiquitous digitalization brings numerous advantages, it also opens the door to new types of threats. The increasing amount of sensitive data and key services stored and processed online makes systems vulnerable and there is an increasingly pronounced need for stronger forms of protection. This is why cybersecurity has become one of the main challenges of the modern era and the foundation of the security and stability of modern society. Critical infrastructure, such as energy, transport and communication systems, represents the fundamental support for the everyday functioning of society and is particularly vulnerable to security threats. Their protection is crucial for the stable functioning of the state, because cyberattacks on sectors such as transport, energy and communication can have serious consequences for society, such as economic, political and security crises. Therefore, the protection of critical infrastructure must not be left to chance. It is necessary to develop comprehensive security strategies that include modern technology, the legal framework and international cooperation. Regular employee training is also necessary so that they are aware of the risks and implications and are prepared to solve problems.

Keywords: cyber threat; digital security; web threats.

1 Introduction

In today's society, heavily reliant on technology, securing data and IT systems is becoming increasingly important. Cybersecurity is no longer the privilege of large corporations or government agencies – today, all users, regardless of social or economic status, are potentially exposed to digital threats. While security technologies are continuously developing, methods of cyberattacks are advancing at the same, if not faster, pace. Many countries, regardless of the level of technological development, have already established digital measures to protect vital infrastructure, which confirms the necessity of preventive action in cyberspace. Protecting critical infrastructure requires constant improvement of systems for detecting and combating threats. Monitoring and control technologies play a crucial role because they enable precise control over production and distribution processes, for example, electricity.

Although security has been present throughout human history, it only became the subject of serious scientific analysis during the 20th century. Traditionally, it was associated with military power and state defense, but after the end of the Cold War, the focus expanded to

individual security, resulting in the development of the concept of human security. The terrorist attacks of September 11, 2001, further redefined the understanding of threats, blurring the line between internal and external threats. This prompted Western countries to revise security policies and adopt new strategies for protecting citizens and institutions. In this context, cybersecurity is becoming a key element of national security and a necessary prerequisite for the stable functioning of modern society and economy (Jarža, 2022). Cybersecurity has recently reached a new level of importance, becoming crucial for digital business. With the development of digital technologies, new approaches and methods of protection appear, while on the other hand, hackers are constantly developing new tools and techniques for breaking through security frameworks (Kaur, Ramkumar, 2022). The primary goal of cybersecurity is to preserve the digital environment, protect user data, and prevent unauthorized access through clearly defined security protocols and regulations (Jarža, 2022). Given the modern world's strong dependence on electronic technology, protecting data from cyberattacks has become an extremely demanding and important task. It also requires additional investment and caution (Li, Liu, 2022). Cyberattacks most often aim to cause financial damage to companies, but in some cases their purpose can also be military or political in nature. Cyberattacks can cause serious financial losses and damage a company's reputation. For this reason, strong defense in the digital space has become a key element of business resilience. Many organizations today establish special cybersecurity teams, responsible for identifying, preventing, and responding to digital threats (Jarža, 2022).

2 Threats And Risks Of Cyberattacks

Cyber threats are now considered a serious threat to national security (Jarža, 2022). They represent one of the most serious challenges of the modern digital age. Their impact is far-reaching – from jeopardizing the operations of private companies to undermining national security. Such attacks can seriously jeopardize business. More than half of small businesses cease operations within six months of an attack. Financial damage is often significant, and the company's reputation can be permanently damaged. Protection against attacks must include both prevention and recovery plans. Information security is crucial for business success today (Toth, 2022). The motives of attackers can be diverse – from entertainment, to crime, to political goals. Over time, terrorist organizations have begun to use digital attacks to attack military and state targets (Jarža, 2022). Attacks often involve blackmail – attackers encrypt data and demand money to unlock it. In addition, attacks can cause stock prices to fall and legal problems with users or partners. To avoid this, companies need to understand what threats they face and how they can defend themselves. Today, attacks via mobile phones, smart devices and other unprotected systems are common. Unfortunately, many companies still do not have sufficient protection. with the danger of physical and virtual attacks, it is important to recognize new types of threats in time (Toth, 2022).

For successful defense, cooperation between the state and private sectors is necessary. Only through joint efforts is it possible to create a safe environment for work and life. With the constant threat of physical and digital attacks, it is necessary to understand new threats and ensure cooperation (Antunović, 2024). Good defense starts with knowledge – understanding what cybersecurity is and how to react when a problem occurs. The key is to develop resilience – being ready before, during and after an attack, which should be part of a broader business strategy. Namely, the realization that an attack is always possible allows you to prepare in time and defend yourself better (Toth, 2022).

2.1 Types of cyber attacks

According to Uzelac (2024), cyber terrorism includes attacks based on digital technologies with the aim of disrupting key functions of society. The most common forms are malware, ransomware, DDoS attacks, phishing and botnet networks. Attacks such as NotPetya and WannaCry have caused global disruptions and major economic losses, while attacks on CARNet, KBC Zagreb and HZZO have been recorded in Croatia. DDoS and ransomware attacks particularly threaten healthcare, education and state institutions, while phishing and pharming use fake messages and websites to steal user data. Cyber threats are becoming more frequent and technically advanced, especially against critical infrastructure such as energy networks, telecommunications and financial systems (Antunović, 2024). In addition to intentional attacks, there are also natural threats such as earthquakes and floods, as well as technical and accidental threats arising from human errors or system failures (Antunović, 2024). To effectively defend against cyber threats, it is necessary to develop a comprehensive security strategy that includes preventive measures, early detection systems, and recovery plans (Toth, 2022). Data encryption, multi-factor authentication, firewalls, and ongoing employee education to recognize threats such as phishing and social engineering play a key role (Šabić, 2023). Resilience to cyberattacks should be an integral part of business planning to reduce risks, prevent business interruptions, and maintain user trust.

3 Techniques And Tools For Preventing Cyber Threats

Cyber threats are becoming an increasing challenge in modern society. This is especially evident in recent decades, when many key systems have become digitalized and connected via computer networks. Such connectivity opens up space for various forms of cyber-attacks. The consequences of these attacks can be serious and affect numerous levels – from individuals, to companies, and even countries. The damage can be financial, informational, and even security in nature (Uzelac, 2024). In the early stages of computer development, security was not the focus because they were used exclusively by scientists and engineers for research, without worrying about misuse. It was only in the late 1980s that it became clear that systems and networks needed to be protected. Security solutions gradually developed, and encryption became key to data protection. With the emergence of viruses and other threats, the antivirus and security software industry was born. However, the sophistication of the attacks required constant adaptation of tools, which brought technical and financial challenges. Due to the increasing incidence of digital fraud and theft, countries have begun to encourage a more serious approach to cybersecurity, although many companies have long considered security an unnecessary expense (Mataić, 2022).

One of the key challenges is that cyber threats do not have geographical boundaries, which makes their identification and control difficult. Also, these threats are often complex, multidimensional, and targeted at critical networks and infrastructures, making them extremely destructive. Traditional methods such as the military and police are not sufficient to combat them; effective cooperation between the public and private sectors that share common interests in protecting against these threats is necessary (Li, Liu, 2022). Therefore, there is an increasing need to strengthen protection systems and develop effective countermeasures. In order for defense to be successful, it is important to understand the ways in which attackers operate. It is necessary to know what methods they use, what tools they use, and how their tactics change. Advanced software tools and security technologies play a major role in this. They enable earlier detection of threats and faster response to potential attacks. It is important to continuously identify security weaknesses, introduce technical protection measures and

constantly improve the system. There is no single solution for complete security. Regular user education, security checks and adaptation to new forms of threats are required. The human factor plays a major role – both intentional actions and unintentional errors can lead to security incidents. As attacks become increasingly complex, protection against cyber threats is becoming the main task not only of states, but also of private companies and other organizations around the world. Various models of defense and security solutions are available that help reduce the risk of cyber terrorism and preserve key infrastructure (Uzelac, 2024).

Choosing a suitable information system and taking care of its security are key to the successful operation of any organization. These elements directly affect the stability and efficiency of business processes. However, it is not enough to just set up and protect the system – its operation must be monitored regularly. In this way, a balance can be maintained between functionality and an acceptable level of risk that does not endanger business (Toth, 2022).

One of the most important ways to protect against cyber threats is to systematically educate employees and raise awareness of the dangers posed by cyber-attacks. In modern security frameworks, employees are increasingly seen as the first line of defense, and not just as system users. Threats such as phishing, spear-phishing, pretexting and other forms of social engineering target human weaknesses – curiosity, carelessness or insufficient understanding of security procedures. In these situations, attackers do not look for technical failures, but exploit human error as the fastest and most effective way to compromise the system (Uzelac, 2024). Regular training and exercises have been proven to reduce the risk of unauthorized access to systems, and successful educational strategies often include simulated attacks so that employees can practice recognizing threats in a controlled environment (Uzelac, 2024). The combination of technical innovation, continuous employee education and a responsible security culture creates the strongest and most reliable defense against sophisticated cyberattacks, and at the same time promotes the resilience of organizations and countries to the challenges of the digital age (Thakur, et al, 2015).

3.1 Firewalls as basic protection

Firewalls are a fundamental tool for protecting computer networks. They serve as barriers between the internal network and the Internet, filtering incoming and outgoing traffic according to security rules (Uzelac, 2024). These are intrusion detection systems, intrusion prevention systems, and encryption. Together, these technologies form a multi-layered protection (Rupić, 2024). Their goal is to block potentially harmful data, allowing only secure communications (Uzelac, 2024). They enable timely detection of threats, prevent attacks, and preserve the integrity of network systems. (Rupić, 2024). Firewalls examine data packets and decide whether to forward or block them, using rules set by the administrator. These rules include IP addresses, ports, protocols, and other network characteristics (Uzelac, 2024). IDS recognizes suspicious activities, while IPS actively stops attacks. Encryption protects data privacy (Rupić, 2024).

There are several types of firewalls, which differ in their mode of operation, level of protection and performance. By choosing the right type of firewall, it is possible to achieve the optimal balance between security, speed and complexity of network management.

3.2 IDS/IPS systems (attack detection and prevention systems)

IDS and IPS systems are essential for monitoring network traffic and identifying potentially malicious activities. IDS systems have a detection role – they recognize suspicious actions and alert the administrator, without direct intervention (Uzelac, 2024). IDS monitors network traffic and system operation, with the aim of detecting deviations, suspicious behavior or possible intrusion attempts. There are two main types of these systems. Network-based IDS (NIDS) focuses on monitoring traffic within the entire network, while Host-based IDS (HIDS) monitors activities and changes on individual computers or servers. IDS systems use a combination of different methods – from recognizing known attacks based on signatures, to analyzing unusual behavior patterns. When they detect a threat, the systems can generate an alert and notify the administrator, enabling a quick response (Mlinar, 2023). On the other hand, IPS systems actively respond to threats and can automatically block malicious activities, for example by terminating the connection to a dangerous IP address (Uzelac, 2024). Although they have similar functionalities, the main advantage of IPS is its ability to take preventive action in real time, which reduces the possibility of system compromise (Mlinar, 2023). These systems use two basic methods for identifying threats: the first is detection based on known attack patterns (signature-based), and the second is analysis of deviations from normal behavior (anomaly-based). A well-known example of such software is Snort, which combines both methods and offers a high level of customization. Thanks to the large number of available rules, Snort is used to detect various types of attacks and adapts to different security environments (Uzelac, 2024). While a firewall is considered the first layer of defense because it filters traffic and blocks unwanted access, what it misses, the IDS should register. It is important to note that neither firewalls nor IDS systems are infallible – advanced attackers can still find a way to bypass protection and exploit system vulnerabilities (Mlinar, 2023).

3.3 Encryption solutions

Encryption is crucial for protecting sensitive information in the digital world. It ensures that data remains unreadable to anyone who is not authorized, even if they manage to intercept it during transmission or storage. Regardless of the circumstances, encryption protects the confidentiality and integrity of data. There are two main categories of encryption that are most commonly used:

1) Symmetric encryption

This method uses a single shared key for both processes – both for encrypting data and for returning it to its original form, i.e. decryption. Its advantage is high speed and high efficiency, which makes it suitable for processing large amounts of data, for example in backups, databases or communication within closed networks. However, the security of the system depends entirely on the way the key is exchanged between the participants. If the key falls into the wrong hands, the entire system can be compromised, because the attacker then has access to all encrypted data. An additional challenge is the need for a secure channel or protocol for key transfer, which in practice often requires combining with asymmetric methods to achieve greater security (Uzelac, 2024).

2) Asymmetric encryption

Unlike the symmetric method, this method uses a pair of cryptographic keys - a public key, which is freely shared and used for encryption, and a private key, which remains secret and

serves to decrypt data. This method is slower due to more complex mathematical operations, but it enables the secure exchange of keys over insecure communication channels, such as the Internet, without the need for prior agreement on a secret key. Asymmetric encryption is often used in digital signatures, authentication and protection of electronic mail, and an example of the most famous algorithm is RSA. Its security is based on the mathematical complexity of problems such as the factorization of large numbers, which makes it resistant to most conventional attacks, although future developments in quantum computing may change the security picture (Uzelac, 2024).

3.4 Antivirus software, vulnerability analysis tools and SCADA

Antivirus and antimalware programs specialize in detecting, preventing, and removing various types of malicious software that can compromise the security of computers and networks. They not only recognize known virus and malware patterns, but also use advanced techniques such as heuristics, which allow the identification of new and unknown threats based on suspicious program behavior. They also analyze how software behaves during operation, which helps detect sophisticated and hidden threats that traditional signatures may not immediately recognize (Uzelac, 2024).

Vulnerability analysis allows the detection of security flaws in applications and systems that may present an opportunity for attackers. Using various tools, systems are scanned and compared against databases of known security flaws. In addition, security settings are checked to identify possible weaknesses. This process helps administrators detect threats in a timely manner and remove them, thereby reducing the risk of attacks and damage (Uzelac, 2024).

SCADA systems are a key part of industrial control systems that manage critical infrastructure such as energy networks, water supply and transport. Their main task is to collect and process data in real time, which enables automation and efficient control of complex processes. Recently, they have increasingly been connected to IT networks and use Internet protocols, which brings them advantages in speed and availability, but also increases exposure to security threats. Since they have to work continuously, security updates are often delayed, and many devices do not have the capacity for classic protection tools such as antivirus. Remote access, open protocols and previous neglect of security aspects further increase the risks. Therefore, the security of SCADA systems is today not only a technical, but also a strategic challenge (Mataić, 2022).

4 Cyber Security Of Critical Infrastructure

Modern societies increasingly depend on the proper functioning of critical infrastructures. Critical infrastructures produce and distribute essential products or services, such as energy transmission systems, water purification and distribution infrastructures, transportation systems, communication networks, nuclear power plants, and information technologies. Critical infrastructures refer to the fundamental systems, facilities, and networks that are essential for the functioning of modern society. (Antunović, 2024). Becoming resilient is becoming a key feature for critical infrastructures, which are constantly exposed to threats that can jeopardize security and business continuity (Cantelmi, et al. 2021). The European Defence Fund 2021-2027 is addressing both improving cyber defence and incident management with artificial intelligence and improving efficiency of cyber trainings and exercises (Furlić and Leško, 2021). Especially in recent years, attacks on critical infrastructures, critical information infrastructures, and the Internet have become increasingly frequent, complex, and targeted (Lehto, 2022). Critical

infrastructure actually includes assets, systems, facilities, networks, and other resources on which the functioning of society depends, and which are of crucial importance for preserving national security, economic stability, and public health and safety. For example, the electricity that powers our homes, the water we use, the transportation that enables our movement, the stores where we shop, and the digital communications that enable us to connect with family, friends, and colleagues. It is crucial to recognize which infrastructure must remain operational to ensure the continuity of essential services and which is most vulnerable to threats or hazards (Mataić, 2022).

The importance of critical infrastructure lies in the fact that these systems are the backbone of modern society and without them, everyday life would come to a standstill (Antunović, 2024). The four key functions of life – transport, water, energy, and communications – are so important that the interruption or disappearance of any of them would directly affect the safety and stability of critical infrastructure in different sectors. These interconnections between infrastructure elements mean that the loss of one function can cause a domino effect, affecting other sectors. Therefore, over time, a chain loss of other functions can occur (Mataić, 2022). Critical infrastructures are interdependent, meaning that they need each other to function successfully. For example, the transport system depends on the energy sector for its energy source, while the transport system is used to deliver fuel to the energy sector. The failure of one critical infrastructure can have a cascading effect on other essential infrastructures, causing huge consequences and financial loss (Antunović, 2024). Identification and recognition of sectors of critical importance and their inter-sectoral connections allows for better cooperation and data exchange, thus contributing to the sustainability of businesses and services (Mataić, 2022). The following sectors stand out in particular: energy, transport and telecommunications due to their key impact and interdependence with other sectors.

Cyber incidents most often occur in three main areas. The first is the exploitation of security flaws and vulnerabilities in mobile devices, the second is impersonation to steal personal data and identity, better known as phishing, and the third is the manipulation of employee weaknesses within an organization. Although employees are recognized as a crucial factor in the successful or unsuccessful management of information security, the number of security incidents caused by human actions is increasing year by year (Arbanas, 2020). Practical examples show how serious the consequences of such attacks can be. One of the more famous cases occurred in Ukraine at the end of 2015, and was repeated a year later. A cyber attack on three electricity distribution companies caused a power outage for several hours, leaving around 225,000 people without power. According to available information, months earlier, using targeted phishing messages, attackers managed to enter internal networks, collect security credentials and study the system structure in detail so that they could carry out the attack at the right moment (Arbanas, 2020). Another well-known example is the Stuxnet malware attack, which managed to physically damage centrifuges at an Iranian nuclear power plant. Of particular concern is the fact that this system was not connected to the internet, but the attackers still found a way to take control of Siemens programmable logic controllers (PLCs) and thus cause great damage. Croatia is not spared from such threats. Among the more well-known domestic examples are the phishing attacks on state and public institutions in 2018. The most notable case was the case from Đakovo, where a city administration employee, believing that he was acting on instructions from the mayor received via email, transferred 50,000 euros to the account of a person named John Smith without additional verification. Another attack that attracted a lot of public attention was the one on INA d.d., which began on Valentine's Day 2020. The attack, which lasted several days, was classified as

a DoS, and official details of its scale and consequences were never fully disclosed (Arbanas, 2020).

Also, in late September 2015, there was a major failure in the T-com network. At one point, both landline and mobile telephony disappeared, and the internet stopped working completely. This was not just a technical problem – the consequences quickly spread to everyday life and key services. The national emergency service 112 became completely unavailable, which meant that citizens could not get help in the event of an accident, fire or medical emergency. At the same time, systems for internal POS transactions in shops and branches stopped, and international payment exchange via the SWIFT network was disabled, paralyzing part of the banking system. The problems did not stop there – until 13:00, serious difficulties or a complete shutdown of operations affected the Zagreb Stock Exchange, the Croatian Health Insurance Institute, the Croatian Post, the Tax Administration and numerous other state and private entities that depend on stable telecommunications connections for their operations. That day, many realized how interconnected all segments of modern society are – from healthcare and finance to trade and public administration. Although the cause was not a hacker attack, but a technical failure, this incident clearly showed how vulnerable critical information infrastructure is. It also served as a warning that it is necessary to invest in its better protection, maintenance and resilience in order to prevent similar situations that could have even more serious consequences in different circumstances (Kezerić, 2017).

A common element is clearly visible from these cases – the human factor. Whether it is an oversight, lack of knowledge or conscious action, people are often the weakest link in the security chain. This once again confirms the need to pay special attention to education, awareness, and building a security culture among employees when planning an information security management strategy (Arbanas, 2020).

4.1 Ways to deal with cyber threats in critical infrastructure

Addressing cyber threats to critical infrastructure requires a comprehensive approach that includes collaboration between the public and private sectors, ongoing user education, and the implementation of advanced technologies for threat prevention and detection.

Key aspects include regular updates of security measures, vulnerability management, authentication, and a layered network architecture that reduces exposure to attacks. In addition to technical measures, it is important to establish effective coordination between all relevant stakeholders, such as government agencies and private organizations, and to build trust through timely information exchange and joint decision-making (Rashid, et al, 2019).

It is necessary to develop effective strategies, policies, and priorities for the protection of critical information infrastructure (CII), also known as CIIP. Although CIIP is considered part of the broader concept of critical infrastructure protection (CIP), the difference is that CIP is a matter of national security, while CIIP has a broader, global significance. It is therefore crucial that governments and the private sector work together to strengthen partnerships, especially in the area of information exchange and joint response to threats. CII as a fundamental component of digitalized infrastructure requires special attention, as any serious disruption in its operation can jeopardize the security of the entire country (Roshanaei, 2021). European projects aimed at strengthening the cybersecurity of critical infrastructure are developing a number of innovative tools and approaches. Examples include Critical-Chains, which uses blockchain and IoT technologies for safer financial transactions, with an emphasis on multi-layered protection and privacy. FINSEC is an EU project that developed an integrated platform for predictive and collaborative security of financial infrastructures,

combining cyber and physical protection. Its aim was to improve threat detection and prevention using artificial intelligence, risk analysis and information exchange between financial institutions. It brings an integrated model of cyber and physical protection in the financial sector. PANACEA is an EU project that develops tools for monitoring and assessing the physical and cognitive state of commercial drivers to increase road safety. The project provides cloud-based solutions for drivers, operators and supervisory institutions, tested through realistic pilot scenarios. focuses on the healthcare sector, combining technical and non-technical tools for the security of medical systems and personnel. ReAct is an EU project that develops advanced methods for timely detection and mitigation of cyber threats through active network scanning, automatic blocking and isolation of compromised systems. The goal is to increase the security of IT infrastructures by predicting and reacting to security incidents. The RESISTO platform is an EU project that develops a platform to strengthen the resistance of communication infrastructures to cyber, physical and natural threats. The platform combines advanced technologies such as blockchain and data analytics to improve risk management and situational awareness (Roshanaei, 2021).

5 Conclusion

Cybersecurity has become a key element in protecting the digital space and preserving the stability of modern society. The development of digital technologies brings numerous advantages, but also new threats that are increasingly complex and demanding to defend. The protection of data, systems and infrastructure is essential for preserving stability and trust in the digital society. Organizations and states are increasingly investing in security measures, more precisely in specialized teams and technologies in order to successfully cope with these challenges and maintain the trust of citizens. Cyber terrorism represents a special danger, which not only threatens financial losses, but also destabilizes social and political systems.

Attacks aimed at critical infrastructure, such as healthcare, energy and transport, clearly show how vulnerable the system is. For example, in Croatia, incidents at key institutions have highlighted the need for better coordination and rapid responses by security services. In addition to technical measures, user education and awareness-raising play an important role in reducing risks and strengthening resilience to cyber threats. The application of new technologies such as the Internet of Things and artificial intelligence opens up opportunities, but also requires new approaches to defense.

Cooperation between the public and private sectors is essential for successful threat management. European projects and innovative solutions provide guidelines for improving protection, and legal frameworks, such as the GDPR and others, provide the basis for data regulation and protection. However, security systems must be flexible and adapt quickly to keep up with technological changes. The development of the legislative framework and investment in the development of a security culture among users further strengthen the resilience of society. Ultimately, the security of the digital space is not just a technical challenge, but a joint task of all actors in society.

Protecting critical infrastructure is a special and complex task because its functionality ensures the work of many other sectors. Croatia and other countries face challenges in this area, but through technological innovation, modernization of security protocols and cross- sector cooperation it is possible to build more resilient systems. Only by continuous investment in technology, people and strategies can stability and security be ensured, which is crucial for national development and prosperity. Cyber security today is not a luxury, but a necessity that protects not only data, but also the fundamental values of modern life.

References

Antunović, J. (2023) 'Sigurnost komunikacije u kritičnoj infrastrukturi' (thesis). Zagreb: *Sveučilište u Zagrebu*, Fakultet prometnih znanosti (accessed 05/10/2025) https://zir.nsk.hr/islandora/object/fpz:3050

Arbanas, K. (2020) 'Ključni čimbenici kulture informacijske sigurnosti' (accessed 08/13/2025) 4-20-7.pdf

Cantelmi, R., Di Gravio, G. and Patriarca, R. (2021) ' Reviewing qualitative research approaches in the context of critical infrastructure resilience'. *Environmental Systems and Decisions*, 41(3), 341–76.

DeepWork Capital (2023) 'Understanding Cybersecurity: The Role of Human Behavior and Psychological Security in the War Against Online Manipulation' (accessed 05/10/2025) https://www.deepworkcapital.com/understanding-cybersecurity-the-role-of- human-behavior-and-psychological-security-in-the-war-against-online-manipulationt

Direktiva 2022/2555 Europskog parlamenta i Vijeća (2022) 'Direktiva NIS 2 o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije'. https://digital-strategy.ec.europa.eu/hr/policies/nis2-directive

Furlić, J., and Leško, L. (2021) 'Research and development trends in the field of defence: European defence fund'. *Global Journal of Business and Integral Security*, 4(3).

Geron, T. (2013) 'Airbnb and the unstoppable rise of the share economy'. Forbes. URL: http://www.forbes.com/sites/tomiogeron/2013/01/23/airbnb-and-the-unstoppable-rise-of-the-share-economy/.

Grgec, Ž. (2023) 'Pravni aspekti regulacije interneta stvari na tržištu elektrotehničkih komunikacija RH' (thesis) *Zagreb: FER.* https://repozitorij.unizg.hr/islandora/object/fer:11974

Jarža, I. (2022) 'Kibernetička sigurnost kao komponenta koncepta korporativne sigurnosti' (thesis). Zagreb: FPZG. https://repozitorij.unizg.hr/islandora/object/fpzg:1702

Kaur, J. and Ramkumar, K. R. (2022) 'The recent trends in cyber security: A review'. *Journal of King Saud University – Computer and Information Sciences*, 34(8), 5766–81.

Khadka, K. and Ullah, A. B. (2025) 'Human factors in cybersecurity: an interdisciplinary review and framework proposal'. *International Journal of Information Security*, 24(3), 1–13.

Kezerić, A. M. (2017) 'Analiza prijetnji i rizika cyber sigurnosti Republike Hrvatske: ranjivost informacijske infrastrukture '(thesis) Zagreb: Sveučilište u Zagrebu, Fakultet političkih znanosti.

Keepnetlabs (2024) 'The Complexity of Human Behavior in Cybersecurity'. https://keepnetlabs.com/blog/the-complexity-of-human- behavior-in-cybersecurity

Lehto, M. (2022) 'Cyber-attacks against critical infrastructure'. *In: Cyber Security: Critical Infrastructure Protection. Cham: Springer*, pp. 3–42.

Li, Y. and Liu, Q. (2021) ‘A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments’. *Energy Reports*, 7, 8176–86.

Mataić, I. (2022) ‘Cyber security – zaštita kritičnih infrastruktura’ (thesis) *Koprivnica: Sveučilište Sjever.*

Mlinar, D. (2023)’Sustavi za detekciju i prevenciju upada u računalne sustave’ (thesis) *Virovitica: Veleučilište u Virovitici*.

Noonan, L. (2025) ‘Understanding Human Behaviour to Strengthen Security’. *Cyber Security Awareness Metablog.* Metacompliance. https://www.metacompliance.com/blog/cyber-security-awareness/understanding-human- behaviour-to-strengthen-security

Presido (2021) ‘ Personal Information Protection Law (PIPL)’ https://presido.hr/blog/personal-information-protection-law-pipl-novi-kineski-zakon-o-zastiti-osobnih-podataka-97/

Rashid, A., Danezis, G., Chivers, H., Lupu, E., Martin, A., and Lewis, M. (2019) ‘Scoping the cyber security body of knowledge’. *IEEE Security & Privacy*.

Roshanaei, M. (2021) ‘Resilience at the core: critical infrastructure protection challenges, priorities and cybersecurity assessment strategies’. *Journal of Computer and Communications,* 9(8), 80–102.

Rupić, Ž. (2024) ‘Implementacija sigurne mrežne arhitekture’ (thesis) *Šibenik: Veleučilište u Šibeniku.*

Sahufan, M. H. M. and Abesekara, R. (2023) ‘A Comprehensive Framework for Organizational Decision-Making for Managing the Socio-Technical Human Aspect of Cyber Security’. Sahufan_Kariapper_UOG_S4311249_Human_Factors_assignment_CT7098-libre.pdf

Šabić, M. (2023) ‘Ugroze u kibernetičkom prostoru’ (thesis) *Split: Sveučilište u Splitu.*

Thakur, K., Meikang, Q., Keke, G. and Liakat. M. A. (2015) ‘An investigation on cyber security threats and security models’. *IEEE International Conference on Cyber Security and Cloud Computing.* https://ieeexplore.ieee.org/abstract/document/7371499

Toth, J. (2022) ‘Informacijska sigurnost i zaštita poslovanja od kibernetičkog napada’ (thesis). *Varaždin: Sveučilište Sjever.*

Uredba (EU) 2016/679 Europskog parlamenta i Vijeća (2016) ‘Opća uredba o zaštiti podataka’ (GDPR). Službeni list Europske unije, L 119/1. https://www.zakon.hr/z/3112/opca-uredba-o-zastiti-podataka---uredba-%28eu%29-2016-679-

Uzelac, A. (2024) ‘Računalna forenzika za internet’ (thesis). *Rijeka: Sveučilište u Rijeci*