Vesić Slavimir[*]
https://orcid.org/0000-0003-2020-8418
Bjelajac Martin[**]
https://orcid.org/0009-0005-0982-3454

UDK: 343.9:004.738.5
Original scientific paper
DOI: 10.5937/ptp2302077V
Received: 26.04.2023.
Approved on: 23.05.2023.
Pages: 77–88

CYBER SECURITY OF A CRITICAL INFRASTRUCTURE

ABSTRACT: A critical infrastructure consists of basic assets and facilities whose functioning has a significant impact on the society and economy of a country, as well as on its security. The life and work of the citizens of a country are largely dependent on a smooth operation of various energy, telecommunication, water and sewage facilities, as well as the network of hospitals and health institutions, transportation, etc. The safe functioning of these systems is a prerequisite for the existence and development of a social community in an area. Therefore, it is necessary to undertake all necessary activities to preserve a critical infrastructure both in reality and cyberspace. With the development of the Internet, there has been a transformation of people's work and life in the broadest sense, in such a way that it has become an indispensable part of everyday life of each of us. Together with the largest global network increasingly used as well as the various services people necessarily being relied on in the new reality the world encountered during the COVID-10 pandemic, there has been created a vast space attracting the malicious users. They act by using the known mechanisms of functioning communication networks and other information technologies, finding the system vulnerabilities and exploit them. In this paper, we will analyze the cyber security of a critical infrastructure, cyber attacks on a critical infrastructure and the measures needed to be taken to mitigate the consequences of cyber attacks.

[*] PhD, PUC "Belgrade Waterworks and Sewerage", Belgrade, Serbia,
e-mail: vesic.slavimir@gmail.com
[**] Harvard University, Cambridge, Massachusetts, United States,
e-mail:martinbjelajac@college.harvard.edu

© 2023 by the authors. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

Keywords: *security, cyber security, critical infrastructure, cyber attacks.*

1. Introduction

For human society to form and remain in a certain area, man adapted the environment to himself with the need to use natural potential and resources, making his life and work easier and more comfortable. The role of infrastructure is multiple and with reason; some authors state that it is a materialized condition for the existence and development of basic human activities in an organized space (Žegarac, 1998, p. 14). In geospace, two groups of networks of infrastructure systems are dominant: social and technical infrastructures. The social infrastructure consists of standard facilities in the domain of health, education, social care, culture, administration, etc. The technical and economic infrastructure consists of networks and facilities: traffic, water management, energy, communications, etc. Each infrastructure branch, or subsystem, with its facilities, network and devices, on the one hand, and organization and functioning, on the other hand, is part of a broader infrastructure system. These are systems of clear and clean connections, where all subsystems can be seen up to the end elements and pronounced vertical connections (Lukić, 2005, p. 5). We are talking about a complex system composed of a large number of other systems, spatially organized, and for that reason, we can consider it as a system of systems where interoperability is its very important characteristic.

Most of the mentioned systems should provide conditions for people's life and work in an area for an extended period of time. Problems in their functioning can produce negative consequences on many different levels: economic, health, security, etc. In modern society, critical infrastructure is managed with the support of information systems and technologies. Most companies that manage critical infrastructure and belong to the technical infrastructure base their IT solutions on many information systems, the main of which are the business information system and the process control system.

The ubiquity of the Internet makes it possible to connect anywhere and anytime, which leads to the increasing use of computers, mobile phones and any device that can connect to the network. This creates such a relationship in which modern society is critically dependent on information as a strategic resource and information and communication technologies, abbreviated ICT (Vesić et al., 2022, p. 91). Cybercriminals and specialized cyber groups find system vulnerabilities and carry out activities aimed not only at financial gain but also many other national, political and social goals through espionage, hacktivism, sabotage and even cyber warfare (Bjelajac & Jovanović, 2013, p. 104).

2. The concept of critical infrastructure

Critical infrastructure is an essential part of the entire infrastructure. If it is temporarily or permanently disabled, it will have far-reaching consequences because many infrastructural subsystems are connected to each other. In a way, it is necessary for the functioning of the economy and society. For example, suppose there is a power outage in an area where pumping stations are located. In that case, it is impossible to distribute water to the population located in a particular altitude zone because the pumping stations will not work. This can further result in an increase in certain diseases and a burden on the health infrastructure due to reduced hygiene. If there is an interruption in the functioning of the critical infrastructure, it will produce cascading effects towards the rest of the connecting infrastructure and disrupt it.

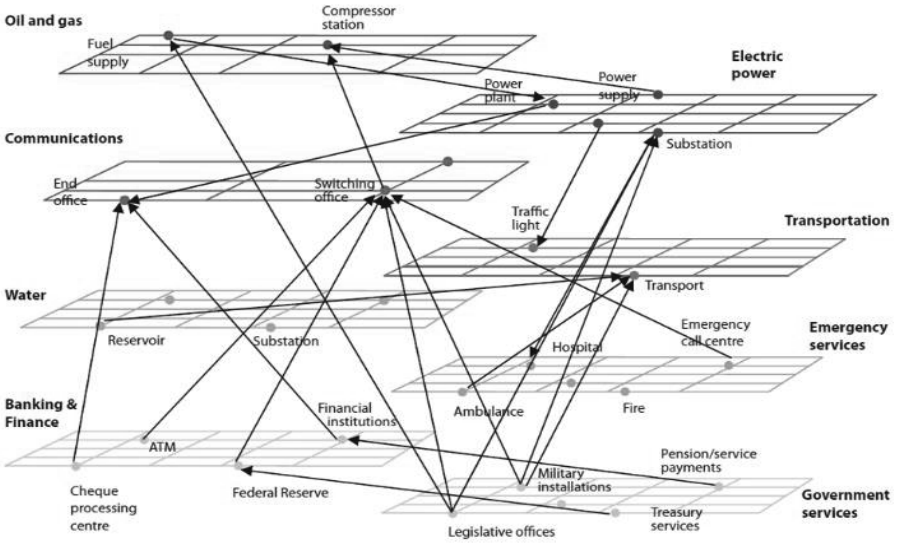
Certain authors state that the concept of critical infrastructure is not easy to define, that there is no widely accepted definition of critical infrastructure and that each country or organization must define its critical infrastructure (Trbojević, 2018, p. 103). For example, Australia defines this term as "those physical facilities, supply chains, information technologies and communication networks, which if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation, or affect Australia's ability to conduct national defence and ensure national security" (Australian Cyber and Infrastructure Security Centre, 2023). In Canada, critical infrastructure "refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. CI can be stand-alone or interconnected and interdependent within and across provinces, territories and national borders. Disruptions of CI could result in catastrophic loss of life, adverse economic effects, and significant harm to public confidence. CI includes both physical and digital infrastructure. Physical infrastructure refers to the built environment, including buildings, vehicles, computer hardware and other assets. Digital infrastructure refers to electronic systems and assets, like data and software" (Public Safety Canada, 2022, p. 22). NIST defines the term as "system and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters (NIST, 2022). The above definitions indicate that there is a difference in the treatment of the concept of criticality in critical infrastructure.

The authors point to two important aspects of critical infrastructure, which over time differentiated the newer definitions of this term (Milosavljević & Vučinić, 2021, pp. 43–44):

- dependency between subsystems – where one subsystem is critical for another if the other must continue working
- critical information infrastructure is a part of critical infrastructure – where if there is an interruption in the functioning of critical information infrastructure, there can be severe disruptions, even a disaster of critical infrastructure, but the failure of critical infrastructure can also occur for other reasons, while the failure of critical information infrastructure is most often a product of cyber attacks (García Zaballos & Jeun, 2016, p. 3)

Figure 1 shows the interdependence of critical infrastructure. If disruptions occur in one sector, it is transmitted to other related sectors through a ripple effect; thus, certain areas can remain completely paralyzed. Therefore, another important aspect of the infrastructure is its recovery.

Figure 1. Utility and network interdependencies



Source: OECD (OECD, n.d.)

Figure 1 shows the interdependence of critical infrastructure. If disruptions occur in one sector, it is transmitted to other related sectors through a ripple effect; thus, certain areas can remain completely paralyzed. Therefore, another important aspect of the infrastructure is its recovery.

For the successful management of critical infrastructure, a group of systems called industrial control systems (ICS) is used, which includes systems with supervisory control and data acquisition (SCADA), distributed control systems (DCS), as well as programmable logic controllers (PLC). They are used in power supply systems, water and sewage systems, oil and natural gas systems, as well as in chemical, pharmaceutical and discrete production, etc. (Stouffer et al., 2015, p. 1). With the development of the Internet, there is a need for a greater number of different types of information systems to be interoperable with each other and with other systems outside the company. ICS integrate with business information systems, and sometimes geographic information systems, to exchange business, industry, and geographic data and create better insights into business using advanced analytics and business intelligence technologies. In addition, there is a need to exchange data with other external systems to consolidate business and obtain better insights, which can be in real-time. As described, systems that are part of critical infrastructure attract various malicious users to conduct cyber operations. If implemented successfully, it can have catastrophic consequences at the national and regional levels, and therefore great attention is paid to the security of these systems.

3. Cyber security

Cyber security is quite a complex term, and there is some ambiguity in what it is due to a large number of definitions of similar terms, such as information security and ICT security. In this context, cyber security can be defined as the protection of cyberspace itself, electronic information, the ICT supporting the space and the users of cyberspace in their personal, social and national capacities, including any of their interests, measurable or immeasurable, that are vulnerable to attacks originating from cyberspace (Von Solms & Van Niekerk, 2013, p. 101). This definition differs from the terms information security and ICT security in that it includes threats not part of the formally defined scope of the other two types of security (Bjelajac & Vesić, 2020, p. 66). Suppose critical infrastructure is exposed to cyber-terrorist attacks. In that case, it is not only a violation of information security through violation of confidentiality, availability and integrity of information, or violation of authenticity, non-repudiation and reliability, but also prevents access to critical services of a country, such as, e.g. electrical network, which reduces the quality of life of its citizens, and in some cases causes lasting consequences for their lives.

Cyber attackers have easier access due to the huge number of individuals who are permanently present on the Internet and exhibit a disorder of addiction to

it (Bjelajac & Filipović, 2020). Individuals and specialized cyber groups appear as cyber attackers. The aforementioned cyber groups, better known as APT groups, are used to achieve various state interests, such as industrial espionage, theft of intellectual property and state secrets, cyber sabotage, destruction of equipment, etc. Their modus operandi is to carry out sophisticated, sustained cyberattacks, better known as Advanced Persistent Threats – APTs, through which a hacker infiltrates a network seamlessly to steal sensitive data over a long period (Crowdstrike, 2023). Compared to traditional attacks, APT attacks are characterized by the fact that: they have precisely defined targets and goals, they are highly organized and well-equipped attackers, they carry out long-term campaigns with repeated attempts, they use stealth and evasive attack techniques (Chen et al., 2014, p. 64). The cyber groups' activities are financed by certain groups or the governments of their countries to achieve their goals through cyber attacks.

4. Cyber security and critical infrastructure

The consequences for infrastructure and people, the long time required for system recovery and the large scale of damage that cyber attacks on critical infrastructure can cause are of concern to countries and organizations that manage them. The history of cyber attacks is characterized by financial losses, the ability to damage physical equipment, and the potential to cause human casualties (Alladi et al., 2020, p. 1). Therefore, it is necessary to pay special attention to the cyber security of critical infrastructure.

We will present some popular cyber-attacks that happened in the last two decades, and before the COVID-19 pandemic, they had a big impact. The first case is the attack on the Davis-Besse nuclear power plant in the city of Ohio in the USA in 2003 when the SQL Slammer worm broke into the private computer network of the nuclear power plant and disabled the security monitoring system for almost 5 hours (Holloway, 2015). Employees were unable to monitor the plant's core temperature sensors, a critical safety hazard at a nuclear power plant. This attack caused a severe incident and pointed to the importance of adequate network configuration and the need to place industrial control systems in a separate network with strict supervision of incoming and outgoing traffic.

Stuxnet is probably the most famous cyber attack, where damage is believed to have been done to Iran's nuclear program at a facility in the city of Natanz. It is a sophisticated malware that was transferred via USB memory into an environment isolated from the Internet and changed how the PLC

controllers that were part of the SCADA system worked. The aforementioned malicious program, knowing system vulnerabilities before the software manufacturer became aware of those vulnerabilities and made appropriate patches to eliminate them, the so-called "zero-day vulnerabilities" (Farwell & Rohozinski, 2011, p. 24), exploited those vulnerabilities. Stuxnet altered the operation of the PLC controllers that controlled the uranium centrifuges so that they rotated at irregular speeds. At the same time, it scrambled the data and presented it to the server as if everything was fine. Since no irregularity in operation was detected, the centrifuges were damaged. When talking about Stuxnet is often referred to as the first cyberweapon.

A cyber attack on a water supply with water treatment plants took place in 2015 in a city in the USA; where due to the sensitivity of the data, the incident was shown under the name KWC – Kemuri Water Company. The attackers concentrated on the weaknesses they found in the company's Web portal. They penetrated the Web payment portal through social engineering techniques such as phishing and SQL Injection attacks. They found credentials to access a SCADA system on an older IBM AS/400 platform there (Vericlave, 2018, p. 3). After that, they changed the level of chemicals used in the water purification process because they had access to different valves that control specific process inputs. There is partially available information about this cyber attack. However, from its scale, as well as the potential damage to the health of water consumers that was done and the fact that about 2.5 million consumer data was leaked, it can be said that it caused severe damage to the state and the lives of its citizens.

The attack on the electricity grid in Ukraine in 2015 was a large-scale attack that caused a power outage for about 225,000 consumers for several hours and prevented the distribution of electricity in the amount of about 73 MWh. The attack took place by taking control of the SCADA system, synergistically acting with a spear phishing attack and installing BlackEnergy 3 malware (Xiang et al., 2017, p. 157). This was followed by other attacks that maintained the intensity of this cyber operation and further compromised ICS operations. In addition to consumer data being stolen through the attack, much of the equipment was damaged during the attack (Alladi et al., 2020, pp. 4–5). After the attack and the significant damage, restoring the system and implementing the necessary measures to prevent the attack from happening again took time.

The COVID-19 pandemic has brought many changes to people's lives and work, called the new reality. In addition to the growth in online platforms for education, online pharmacies and eHealth services, many people have switched to working from home. Natural disasters and crises favour malicious users to launch a greater number of attacks, which also happened in the COVID-19 crisis, where

most of them were aimed at fraud with financial motives, and these were most often attacks aimed at individuals and certain financial organizations. A smaller number of attacks were directed at facilities and networks of critical infrastructure, but they also occurred primarily in the domain of healthcare institutions.

The authors (Pranggono & Arabo, 2021, p. 3) cite examples: data on research and patient tests related to COVID-19 were leaked due to a malware attack on a London-based research company, a DDoS attack was carried out on a network of hospitals in Paris that were on the COVID-19 system, a cybercriminal Netwalker forced a university researching a vaccine for COVID-19 to pay a $1.14 million ransom in a ransomware attack.

An analysis of cyber attacks on critical infrastructure in the period from January 2019 to May 2020 found that the most commonly reported attacks were: malware, about 37%; account hijacking, about 17% and targeted attacks, about 10%, with about 85% related to cybercrime and about 11% for cyber espionage, while 1% is cyber warfare (Alagappan et al., 2020, p. 1102). According to IBM's annual reports, the cost of an average data breach on an annual basis increased from 3.86 million dollars in 2020 to 4.24 million dollars in 2021 to 4.35 million in 2022, making it the highest in history. The same analysis shows that the healthcare sector has been the most vulnerable for 12 years, where data breach costs have increased from $7.13 million in 2020 to $9.23 million in 2021, which is about 30%. The trend continued in 2022, where data breach costs amounted to about 10.1 million, 41.6% compared to 2020 (IBM Security, 2021, 2022). All this indicates that the trend of cybercrime growth will continue, and thus the growth of cyberattacks on critical infrastructure.

5. Mitigating cyber attacks on critical infrastructure

Cyber security, as one of its goals, has the mitigation of cyber attacks on critical infrastructure. It is far more realistic to talk about mitigation than to talk about complete prevention because it is about previously researched and analyzed system weaknesses, then well-planned and organized targeted attacks, which are carried out much more often by specialized cyber groups with a clear intention and goal, than by curious individuals whom they work randomly. The measures that need to be taken largely depend on the specific case, but generally speaking, they should go in two mutually complementary directions. One of the measures is technical-technological, aiming to protect information and ICT infrastructure and services. The other part is aimed at the people and raising awareness of a possible cyber attack through specialized training (Stošić & Janković, 2022, p. 92).

Measures of a technical-technological nature include constantly updating security-related software, then periodically checking system vulnerabilities and penetration testing. It is also necessary to enable VPN services to establish an encrypted connection between the employee and the company's server. For greater security and assurance of authentication, it is necessary to implement multi-factor authentication through the scenario that is most suitable for the organization (e.g. code and code from an SMS message). Express the need to introduce a specific security standard, e.g. ISO 27001 and ISO 27002 or a cybersecurity framework such as the NIST CSF. Ensure the company complies with standards and security frameworks through its internal acts. Some authors state that it is very important in the context of cyber security for an organization or enterprise that manages critical infrastructure to use an intrusion detection system (IDS) and a security incident and event management system (SIEM) (Pranggono & Arabo, 2021, p. 5), because they enable timely response. In addition, it is necessary to regularly update the software of the equipment itself as well as the operating systems.

A large number of attacks begin with the placement of various social engineering techniques, so it is necessary to organize specialized training to raise users' awareness of cyber attacks and their level of information security culture. Many cases from practice have shown that even if technical security measures are in place, system vulnerabilities come from people themselves.

6. Conclusion

Critical infrastructure plays a very important role for a country and all individuals who live and work there, so special attention is paid to its security. A large part of that security is cyber security because critical infrastructure includes critical information infrastructure vulnerable to cyber attacks. Attacks are most often organized by specialized cyber groups, which primarily gain financial benefit from such actions because the state or organizations sponsor their activities. Their actions are aimed at national, political or other social goals through industrial espionage, sabotage, hacktivism or cyber warfare operations.

Critical infrastructure is characterized by high interdependence, so the risk of successful cyber attacks is much higher and can produce catastrophic consequences for human lives and the state. Therefore, it is important to act from the state level, towards the organization responsible for managing critical infrastructure, and then towards its employees to the greatest extent possible to mitigate the consequences of such attacks and, in some cases, even prevent them. This implies the joint action of technical-technological measures and measures aimed at the people themselves, i.e. permanent education.

Vesić Slavimir
JKP „Beogradski vodovod i kanalizacija“, Beograd, Srbija

Bjelajac Martin
Univerzitet Harvard, Kembridž, Masačusets, SAD

SAJBER BEZBEDNOST KRITIČNE INFRASTRUKTURE

REZIME: Kritičnu infrastrukturu čine osnovna sredstva i postrojenja čije funkcionisanje ima ogroman uticaj na društvo i ekonomiju jedne države, kao i na njenu bezbednost. Život i rad građana neke države u velikoj meri zavisi od nesmetanog rada raznih energetskih, telekomunikacionih, vodovodnih, kanalizacionih postrojenja, kao i mreže bolnica i zdravastvenih ustanova, prevoza itd. Bezbedno funkcionisanje ovih sistema je preduslov postojanja i razvoja društvene zajednice na nekom prostoru i stoga je potrebno preduzeti sve potrebne aktivnosti radi očuvanja kritične infrastrukture kako u realnosti, tako i u sajber prostoru. Razvojem interneta dolazi do tranformacije rada i života ljudi u najširem smislu na način da je on postao neizostavni deo svakodnevice svakoga od nas. Sa porastom upotrebe najveće globalne mreže, kao i u mnogome oslanjanje na razne servise koji su postali neophodni u novoj realnosti koje je svet zadesio tokom pandemije COVID-19, stvorio se ogroman prostor koji privlači zlonamerne korisnike. Oni deluju na način tako što koriste poznate mehanizme funkcionisanja komunikacionih mreža i drugih informacionih tehnologija, pronalaze ranjivosti sistema i vrše njihovu eksploataciju. U ovom radu analiziraćemo sajber bezbednost kritične infrastruktre, sajber napade na kritičnu infrastrukturu i mere koje je potrebno preduzeti u cilju ublažavanja posledica sajber napada.

Ključne reči: *bezbednost, sajber bezbednost, kritična infrastruktura, sajber napadi.*

References

1. Alagappan, A., Baptist, L. J., Venkatachary, S. K., Samikannu, R., Prasad, J., & Immaculate, A. (2020). Impact of Biological Pandemic in Critical Infrastructure Services – Are We Heading for a Cyber Pandemic? *European Journal of Molecular & Clinical Medicine, 7*(3), pp. 5154–5177

2. Alladi, T., Chamola, V., & Zeadally, S. (2020). Industrial Control Systems: Cyberattack Trends and Countermeasures. *Computer Communications*, 155, pp. 1–8. https://doi.org/10.1016/j.comcom.2020.03.007
3. Australian Cyber and Infrastructure Security Centre. (2023). Defining critical infrastructure. Downloaded 2023, February 26 from https://www.cisc.gov.au/what-is-the-cyber-and-infrastructure-security-centre/defining-critical-infrastructure
4. Bjelajac, Ž. Đ., & Jovanović, M. B. (2013). Pojedini aspekti bezbednosne kulture na Internetu [Certain aspects of security culture on the Internet]. *Kultura polisa, 10*(21), pp. 99–114.
5. Bjelajac, Ž., & Filipović, A. (2020). Internet Addiction Disorder (IAD) as a Paradigm of Lack of Security Culture. Kultura polisa, 17 (43), pp. 239-258
6. Bjelajac, Ž. Đ., & Vesić, S. L. (2020). Security of information systems. *Pravo – teorija i praksa, 37*(2), pp. 63–76. https://doi.org/10.5937/ptp2002063b
7. Chen, P., Desmet, L., & Huygens, C. (2014). A study on Advanced Persistent Threats. In: Decker, B. De & Zúquete, A. (eds.), *Communications and Multimedia Security. CMS 2014. Lecture Notes in Computer Science*, (pp. 63-72), Springer Berlin Heidelberg, https://doi.org/10.1007/978-3-662-44885-4_5
8. Crowdstrike. (2023). What is an Advanced Persistent Threat? Cybersecurity 101. Downloaded 2023, March 10 from https://www.crowdstrike.com/cybersecurity-101/advanced-persistent-threat-apt/
9. Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. *Survival, 51*(1), pp. 23–40. https://doi.org/10.1080/00396338.2011.555586
10. García Zaballos, A., & Jeun, I. (2016). *Best Practices for Critical Information Infrastructure Protection (CIIP): Experiences from Latin America and the Caribbean and Selected Countries*. Inter-American Development Bank
11. Holloway, M. (2015). *Slammer Worm and David-Besse Nuclear Plant*. Downloaded 2023, March 15 from http://large.stanford.edu/courses/2015/ph241/holloway2/
12. IBM Security. (2021). Cost of a Data Breach Report 2021
13. IBM Security. (2022). Cost of a Data Breach Report 2022
14. Lukić, B. (2005). *Uloga infrastrukture u prostornom razvoju Srbije – doktorska disertacija* [*The role of infrastructure in the spatial development of Serbia – doctoral dissertation*]. Beograd: Geografski fakultet, Univerzitet u Beogradu
15. Milosavljević, B., & Vučinić, D. (2021). Odnos prema kritičnoj infrastrukturi u Republici Srbiji [Attitude towards critical infrastructure in the Republic of Serbia]. *Vojno delo, 73*(4), pp. 42-56. https://doi.org/10.5937/vojdelo2104042M

16. NIST. (2022). critical infrastructure. Committee on National Security Systems (CNSS) Glossary. Downloaded 2023, February 20 from https://csrc.nist.gov/glossary/term/critical_infrastructure
17. OECD. (n.d.). Multiple hazards and threats can disrupt critical infrastructure. Downloaded April 21, 2023, from https://www.oecd-ilibrary.org/sites/76326acb-en/index.html?itemId=/content/component/76326acb-en
18. Pranggono, B., & Arabo, A. (2021). COVID-19 pandemic cybersecurity issues. *Internet Technoogy Letters, 4*(2), pp. 1–6. https://doi.org/10.1002/itl2.247
19. Public Safety Canada. (2022). Renewing Canada's Approach to Critical Infrastructure Resilience: What We Heard Report. Downloaded 2023, February 15 from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rnwng-cnd-pprch-crtcl-nfrstrctr-rslnc-2022/rnwng-cnd-pprch-crtcl-nfrstrctr-rslnc-2022-en.pdf
20. Stošić, L. V., & Janković, A. V. (2022). Cybercrime in the Republic of Serbia: Prevalence, situation and perspectives. *Kultura polisa, 19*(4), pp. 82–99. https://doi.org/10.51738/Kpolisa2022.19.4r.82sj
21. Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). Special Publication 800-82 Revision 2 – Guide to Industrial Control Systems (ICS) Security. Downloaded 2023, February 25 from https://doi.org/10.6028/NIST.SP.800-82r2
22. Trbojević, M. (2018). Zaštita kritičnih infrastruktura – iskustva tranzicionih zemalja [Protection of critical infrastructures – experiences of transition countries]. *Politička revija*, *56*(2), pp. 99–118. https://doi.org/10.22182/pr.5622018.5
23. Vericlave. (2018). *The Kemuri Water Company Hack*. Downloaded 2023, February 25 from https://www.vericlave.com/wp-content/uploads/2018/10/Vericlave_WhitePaper_KemuriWater_1018_F.pdf
24. Vesić, D., Sánchez Monroe, J., & Vesić, S. L. (2022). Cyber security and protection against high-tech crime. *Seti IV – Fourth International Scientific Conference – Science, Education, Technology and Innovation*, (pp. 91-98). Belgrade: International Research Academy of Science and Art
25. Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, 38, pp. 97–102. https://doi.org/10.1016/j.cose.2013.04.004
26. Xiang, Y., Wang, L., & Liu, N. (2017). Coordinated attacks on electric power systems in a cyber-physicalenvironment. *Electric Power Systems Research*, 149, pp. 156–168. https://doi.org/10.1016/j.epsr.2017.04.023
27. Žegarac, Z. (1998). *Infrastruktura* [*Infrastructure*]. Beograd. Geografski fakultet: Urbanistički zavod