ALFA BK UNIVERSITY
FACULTY OF INFORMATION TECHNOLOGY
FACULTY OF MATHEMATICS AND COMPUTER SCIENCE
ALFATECH Journal

UDK: 711.45:004.78::343.852
DOI: https://doi.org/10.46793/AlfaTech1.3.22L
Original scientific paper

Cybersecurity of critical infrastructure in smart city

Duško Laković

Abstract: The security of the country, its economy, cities, and their citizens depends on the critical infrastructure, which is the most important part of the total infrastructure. Each subsystem within the critical infrastructure system provides services to other subsystems, and in this sense, they are characterized by a large number of interwoven, tight connections. By maliciously acting on one subsystem, a ripple effect is created that can grow so much that it threatens the security of the state itself. Therefore, the cyber security aspects of critical infrastructure are very important for researchers, government agencies, and professional individuals. The vision of a smart city should enable a better life for all its citizens and humanity as a whole. It presupposes the use of 4.0 technologies such as the Internet of Things, cloud computing, big data, and artificial intelligence. In past, critical infrastructure subsystems have relied to a greater or lesser extent on isolated and proprietary technologies. With the introduction of "things" into those subsystems, a new polygon is created that includes a large number of vulnerabilities that did not exist until that moment.This paper attempts to shed light on the cybersecurity aspects of critical infrastructure in smart city scenarios.

Keywords: cybersecurity, critical infrastructure, smart city, Internet of things, sensors

1 INTRODUCTION

In order to use natural resources and potentials, man has adapted his environment since the earliest communities. That is why every existence of man and society is tied to a certain space. From the spatial aspect, infrastructure implies different spatial, technical and traffic systems as the basis for the functioning of all users of the space and the development of all basic activities in it (Žegarac, 1998, p. 12). In geospace, two groups of networks of infrastructure systems are dominant: social and technical infrastructures (Đurđević, 2009, p. 11). Social infrastructure consists of standard facilities in the domain of: health, education, social care, culture, administration, etc. Technical and economic infrastructure consists of networks and facilities: traffic, water management, energy, communications, etc. Each infrastructural 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 wider infrastructure system. Infrastructure can be seen as a system made up of a number of subsystems, where each subsystem provides clearly defined products and services to other subsystems. Other subsystems use those products and services and perform their core business, and they themselves provide products and services that someone else uses. Each of these subsystems is important for the city and the quality of life of its citizens. The connections between the subsystems are pronounced, strong, and intertwined, and they extend to the level of the entire state and even society as a whole.

Problems in such complex systems can cause negative effects in the economic, social and security fields. Therefore, the previously mentioned connection between them can be a vulnerability that various individuals and specialized groups are ready to exploit and thereby implement their malicious intentions. Each of these subsystems is under the jurisdiction of one or more connected business entities, whose operations are carried out with the use of information technologies. The security of the information systems of the mentioned business entities is very important when we talk about the prevention or mitigation of cyberattacks, because adequate protection of one subsystem protects, to a certain extent, other connected subsystems, and thus the entire country. It is common for each country to provide its own observation and definition of critical infrastructure. Thus, NIST defines US critical infrastructure 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). Therefore, it is very important for each state to define and know what and how to protect.

Global trends in electronics and information technologies have led to a drop in sensor prices and the emergence of a large number of cheap electronic devices, sensors, and microchips that can be embedded in some critical elements and provide data on the phenomenon being observed and monitored. These devices, popularly called "things", use the largest global network - the Internet in order to be able to exchange data, and in some cases even act on the environment itself (i.e., the phenomenon) as actuators. The motive to install them in critical infrastructure facilities is that they enable a better or more efficient solution to specific problems that existed in these complex systems, which could not be solved by the ICT solutions available until then, or could not be solved efficiently enough.

Since the Internet is unsafe, the "things" themselves are under the attack of many malicious users and specialized organizations who want to act on critical infrastructure and therefore on the country whose infrastructure it is (Laković, 2025, p. 55). Since smart cities rely on the operation of "things" to make city services more efficient, they are under constant threat from such attacks. The specificity of these attacks is not only that certain services used by the population will be made unavailable or a part of the IT infrastructure will be unavailable, but some scenarios can be a threat to human life. This primarily refers to those technologies that directly manage vital services for the community, such as water, electricity, traffic, etc. All this provides a new framework in which to look at the security of critical infrastructure.

In the following segment, we will discuss the concept of critical infrastructure. The third part is about smart cities. In the following section, we describe the critical infrastructure elements that are part of smart cities. The fifth unit covers cyber security aspects of critical infrastructure, where we cover practical cases. After that comes the conclusion.

2 CRITICAL INFRASTRUCTURE

Critical infrastructure is the most important part of the total infrastructure and as such requires special attention, relationship and management, because if it is temporarily or permanently damaged, it can produce unfathomable consequences for the state, its security, economy and society as a whole. It is a system of systems, where each subsystem is a whole by itself, but at the same time is a part of the overall system. In this way, a large number of interconnections are realized in one system of systems. Some authors highlight interoperability as a very important characteristic of these large systems (Vesić & Bjelajac, 2023). A connection is established between subsystems by one subsystem requesting certain services from another subsystem, and at the same time the second subsystem provides the requested services to the first. Considering the critical infrastructure as a system of systems and looking at it as a model of interconnected components that are part of a larger whole, allows us to analyze which are the most important services within the critical infrastructure.

As an example, we can look at a scenario where the sewage system uses electricity to transport sewage waste from citizens to treatment plants. Due to the fact that the sewage system, which is a subsystem of critical infrastructure, uses pumping stations in which pumps work, by interrupting the flow of electricity provided by the electrical subsystem, sewage waste cannot be transported to the treatment plant. This can further cause many problems in the health subsystem, as the failure of the sewage subsystem can lead to large scale diseases and epidemics. This further puts pressure on the economic system of a country, which must ensure adequate quality of health services, especially in a situation where it is necessary to preserve a healthy population as long as possible, due to reduced or even negative natural growth, such as in Serbia.

Due to its importance, and the need for a comprehensive approach, it is common for a country to define its critical infrastructure. Therefore, the mentioned term is not easy to define and for now there is no universal generally accepted definition (Trbojević, 2018, p. 3). Some countries, such as the United Kingdom, define critical national infrastructure as “facilities, systems, sites, information, people, networks and processes, necessary for a country to function and upon which daily life depends. It also includes some functions, sites and organisations which are not critical to the maintenance of essential services, but which need protection due to the potential danger to the public (civil nuclear and chemical sites for example)”. In the Republic of Serbia, critical infrastructure is defined by law and consists of those systems, networks, facilities or their parts, the interruption of functioning or the interruption of the delivery of goods or services can have serious consequences on national security, health and lives of people, property, the environment, and the safety of citizens, economic stability, i.e. endanger the functioning of the Republic of Serbia (“□akon o kritičnoj infrastrukturi,” 2018). At the same time, states regulate the criteria by which critical infrastructure is identified (“Uredba o kriterijumima za identifikaciju kritične infrastrukture i načinu izveštavanja o kritičnoj infrastrukturi Republike Srbije,” 2022). All of this speaks in favour of the fact that countries treat critical infrastructure with great care.

According to the authors, critical infrastructure has two important aspects (Milosavljević & Vučinić, 2021, pp. 43–44):

- dependency between subsystems - where one subsystem is critical for another if it is necessary for the other to continue working
- critical information infrastructure is a part of critical infrastructure - where, if there is an interruption in the functioning of critical information infrastructure, serious disruptions can occur, 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 cyber attacks (García □aballos & Jeun, 2016, p. 3)

Bearing in mind that an increasing number of critical infrastructure systems in the modern world rely on the use of information and communication technologies, there is a need to consider them as an inseparable part of critical infrastructure. The authors of this paper also have the above-mentioned point of view.

3 The Concept of Smart Cities

The concept of a smart city does not have a unique name (Cocchia, 2014) or definition (Hollands, 2008) because it has changed over time and has been studied from several aspects and dimensions (Albino et al., 2015), and most generally it refers to a vision in which the city engages its inhabitants and connects the infrastructure electronically (Musa, 2016). It is also described as having the ability to integrate many different technological solutions and manage a wide variety of city assets, which include: local government information systems, schools, libraries, transportation systems, hospitals, power plants, law enforcement and other services in that community. The primary goal of building smart cities is to improve the quality of life of its citizens by using technology that increases the efficiency of services and meets their needs (Musa, 2016). Therefore, the concept of a smart city is inseparable from infrastructure, because they aim to improve the quality of life of its citizens, through effective and efficient infrastructure management.

Achieving the vision of a smart city presupposes the use of the Internet of Things, abbreviated IoT, which is also called the Internet of intelligent devices and represents a radical evolution of the current Internet into a network of interconnected objects that not only retrieve information from the environment but also interact with the physical world through actuation, but use existing Internet standards to provide services for information transfer, analytics, applications and communications (Gubbi et al., 2013). Therefore, smart cities represent one of the main realizations of the Internet of Things technology and that is why their importance is great.

Some authors (Atzori et al., 2010) point out that the basic idea of IoT is the comprehensive presence of various "things" or objects, which includes: RFID tags, sensors, actuators, mobile phones, etc., while others (Borgia, 2014) add virtual/digital entities, which move in time and space, while some (Simić et al., 2016) group everything into intelligent devices: sensors, actuators, microcontrollers and microcomputers. What distinguishes "things" is that they can interact with other "things" and act synergistically to achieve a common goal. The technological and marketing trends that are driving the development of IoT are (Rose et al., 2015):

- ubiquitous connectivity
- widespread adoption of IP-based networking
- computational economics
- miniaturization
- advances in data analytics
- the rise of cloud computing

IoT devices need to send data via the Internet to a server that would process them or, as is more common today, to the cloud. According to NIST: "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.“ (Mell & Grance, 2011). From an economic point of view, cloud computing is often described as turning capital costs into running costs, while some authors believe that the phrase "Pay as You Go" is more appropriate (Armbrust et al., 2010). Cloud computing provides enough resources needed to accept and process the potentially large amount of data that "things" can generate in a relatively short period of time and create analysis and conclusions based on that data with machine learning and artificial intelligence algorithms.

Big data is a term that encompasses the use of techniques for accepting, processing, analyzing and visual presentation of potentially large data sets in a reasonable time frame that is not available with standard IT technologies (NESSI, 2012). Although there is still a vagueness surrounding the concept of big data, these technologies are quite often described in terms of their aspects, which are popularly called V's. Some of them are (Papadokostaki et al., 2017):

- volume - refers to the constant growth of the volume of data generated from different sources and which traditional databases cannot process
- variety - refers to various data collected through sensors, smartphones and social networks
- velocity - it refers to the speed of data acquisition and additionally to the speed with which the data needs to be processed and analyzed
- value - refers to extracting knowledge or patterns from raw data
- veracity - refers to possible unreliability and noise that may be hidden in the data

These three technologies: IoT, cloud computing and big data work together to enable intelligent processing based on certain smart algorithms. On the basis of intelligent processing, it is possible to perform certain business operations that were not possible until that moment using traditional information and communication technologies. The role of artificial intelligence and specifically machine learning, is to enable an increase in the degree of automation through increasing the efficiency of certain business processes. Those business processes are: water reading, recalculation of the shortest route for waste disposal, thereby reducing the harmful effects caused by carbon emissions, etc.

In this way, it is possible to support new or improved business models. In practice, this means enabling a greater degree of business automation, as well as obtaining data in real time about a particular phenomenon that is being monitored, i.e. on the business process whose monitoring is carried out. One important segment is how to integrate this set of technologies with existing traditional ones, which is supported through the hybrid cloud scenario. This is very important for those economic entities that make up critical infrastructure and have a need for geographic data, such as water supply, electricity distribution, public transport, etc. The spatial dimension of these subsystems of critical infrastructure is very important because, based on this information, they can make their processes, especially those related to operational maintenance, significantly more efficient.

4 Smart Cities and Elements of Critical Infrastructure

In practice, it is increasingly common that certain business scenarios regarding critical infrastructure rely on intelligent solutions from the domain of smart cities. These solutions aim to provide efficient management of critical infrastructure, because most often traditional technologies cannot do it or cannot do it cost-effectively, i.e. there is no economic justification. In the example of city water supply systems, SCADA systems are used in the processes of water intake, then later distribution of potable water to consumers. Considering that these traditional systems use expensive sensors, which in some configurations have to be powered by electricity, it is not economically profitable to use them in anomaly detection, because they need to be installed in large numbers. That number is related to the length of the water distribution network, and it can be very large, so the number of these devices can be several tens of thousands.

We mentioned earlier that critical infrastructure systems are interconnected and that elements of one system can use the services of another system. In this way, they depend on the services provided by some other system. One example can be a remote water reading system. IoT modules are installed on devices for reading water consumption, where the data is transferred to the cloud infrastructure in a certain time interval, stored in the database, and later integrated with the traditional information system that deals with the collection of bills for used water. In practice, these modules are based on LoRaWAN and NB-IoT technologies. Both of these technologies are LPWAN technologies and represent very common standardized solutions today. In the context of water supply operations, where there is a need to record water consumption by consumers, IoT modules take over the functionality of water meter readings. In this way, the need to hire people who until now performed the mentioned processes manually, most often with the use of PDA devices, is reduced. This eliminates all reading errors that occur as a result of manual data entry and increases the frequency of readings. It is common for city water utilities to read water meters several times a year and issue bills to consumers based on that. Very often, there are defects in the network that can affect consumption. The frequency of readings makes it possible to remove defects in a much shorter period of time and ensure the correctness of the consumer's account, which significantly reduces the time and resources spent in practice on account corrections.

In the described scenario, after the data is downloaded from the IoT module and ends up in the smart solution database, it can later be transferred to the in-house application or ERP that deals with water invoicing, and in this way, through integration, the implementation of an important business process of the water company is achieved. If, for any reason, the described system fails, then the waterworks will be left without the possibility to generate income based on the water delivered to consumers, which will create a disruption in its operations and thereby endanger all those who use its services, citizens, the economy, and the entire country.

As another example, let's assume that there is a smart solution that monitors the amount of atmospheric precipitation, and depending on that amount of precipitation and the speed with which the sewage drains are filled, flooding of traffic roads may occur. A smart solution based on sensors and the amount of water that exists in the sewer drains is needed to start the business process of notifying the reliable that it is necessary to empty the sewer drains according to a certain priority. When major weather disasters occur, it is an extensive job that needs to be done in a relatively short period of time. If such a smart system fails, then another element of the critical infrastructure is threatened, i.e. its functionality is reduced. In this particular case, traffic roads are less passable and their safety for citizens, emergency services, etc. is reduced.

In the research in Dublin, an intelligent solution was presented that uses several data sources on which it performs analysis: a crowdsensing approach in the analysis of data from social networks, data from the SCATS system and GPS data from city buses (Panagiotou et al., 2016). Based on different algorithms of artificial intelligence that are applied in real time on a large amount of data, anomaly detection is carried out on traffic roads, where it is possible to build a recommendation system based on the mentioned analysis, where there is a crowd and recommend another route from source to destination. Such a system is of crucial importance for many different city services, as well as for the citizens who need to use them, which is mostly the entire population. If emergency services, such as ambulances, firefighters and police, rely on such a system, if it stops working, then serious problems can arise with major security consequences for citizens and society as a whole.

In some industrial cities, air quality and pollution have been a problem for decades, leading to an increase in various diseases among citizens, as well as a strain on health and other social services. For this reason, smart air quality meters are installed and strategically act on the biggest polluters in those cities. If such services were to stop working, the quality of life of its citizens would significantly decrease and return to the period before the described solutions existed.

Based on the presented scenarios from practice, it can be concluded that intelligent systems implemented in smart cities somehow inherit the characteristics of critical infrastructure systems, because they are used in their business processes. If such intelligent systems stop working or their efficiency is reduced, they threaten the operation of other subsystems of the critical infrastructure, regardless of whether they are intelligent or not. Therefore, it is necessary to work on their resilience or provide a backup alternative that can partially or fully take over the function of the required service. That is why the question of the security of such systems is very important, from the level of the individual to the community and all the way to the state.

5 Cybersecurity of Critical Infrastructure Elements in Smart Cities

IoT smart solutions bring efficiency to a company's business processes and the same goes for critical infrastructure. By presenting "things" on the one hand, opportunities for new and better business models open up. On the other hand, a whole new set of problems emerges as IoT devices use the Internet, which is insecure. Therefore, the topic of cybersecurity of IoT devices is very important, especially in the protection of critical infrastructure.

Malicious users exploit vulnerabilities in known communication protocols and the devices that use them and have the ability to conduct attacks that can disable or greatly render inaccurate numerous devices that are embedded in critical infrastructure. The consequences for infrastructure and people, the long time required for system recovery and the large scale of damage that can be caused by cyber attacks on critical infrastructure 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). Below we will describe some examples of cyberattacks on critical infrastructure from practice that involve the use of IoT technologies in smart city scenarios.

In the Netherlands, a group of ethical hackers discovered 6 key zero-day vulnerabilities in Enphase IQ Gateway home solar energy conversion devices (*DIVD-2024-00011 - Six vulnerabilities in Enphase IQ Gateway devices*, 2024; Candan, 2024). The vulnerabilities exist from version 4 to version 8. These vulnerabilities allow hackers to gain complete access and control over a device if the devices connect to the public Internet. The problem is very serious because it is estimated that over 4 million such systems exist in 150 countries and they can be controlled. If the attack is successful, huge losses of electricity and money can occur and therefore pose a significant threat to national security.

In the smart city of Olsztyn, Poland, a cyber attack took place on June 24 and 25, 2023, in which the smart systems that regulated traffic were disabled (RießMarchive, 2023). The attack had its effect on Sprint SA's intelligent transportation system, which adjusts various parameters so that traffic in the city can adapt to changes dynamically and that public transport vehicles have priority. This system includes many elements, such as a traffic management, center traffic intersection monitoring with violation detection, Wi-Fi access points in trams and a weather information system. The attack covered the city center with 96 intersections, including traffic lights whose work was disrupted, as well as other elements of the traffic system. The consequences of the attack are multiple, from traffic jams and congestion on the roads, through the unavailability of ticketing systems in public transport to other dedicated information systems at the service of citizens..

It has been noted that smart homes are a good target for potential attacks and exploitation of their vulnerabilities, as they are constantly connected to the Internet (Das & Gündüz, 2019, p. 125). A DDOS attack can turn off heating and hot water in smart buildings by overloading the building's main control system with traffic.

These are just a few examples of cyberattacks on critical infrastructure elements in smart city scenarios. In practice, there are many more of them and their form changes, as malicious users constantly try to find new ways to implement their intentions. There are a large number of vulnerabilities that IoT "things" bring when they are placed in critical infrastructure, and therefore it is necessary to adequately protect these devices. As the exploitation of vulnerabilities by malicious users is constantly changing, it is necessary to improve protection measures or find adequate alternatives in response to threats coming from the cyber world.

According to some authors, the road to successful implementation of cybersecurity strategies in smart cities requires a combination of technical measures, regulatory frameworks, and collaborative initiatives (Clim et al., 2023). Also, it’s important to be ready for evolution and constant changes in cyber threats.

6 Conclusion

Critical infrastructure, as the most important part of the total infrastructure, is characterized by a large and rigid interconnection of the subsystems that make it up. Business entities that manage critical infrastructure use information and communication technologies in their operations. Smart cities are a vision of a modern society in which people's lives are improved and sustainability is improved through intensive data exchange of various infrastructure elements, which makes the services that people use better.

In order to achieve this, "things" are built into the critical infrastructure. Considering that they use the public Internet, they come under the attack of malicious users from cyberspace, who want to exploit their vulnerability. If there is a cyber attack and exploitation of vulnerabilities, it does not mean that only the element of the infrastructure on which the attack took place will be disabled, but perhaps also other connected elements of another subsystem. In this way, a wave effect is created that produces cascading effects in which one part of the larger infrastructure can be disabled and the life of the inhabitants of the city and the country threatened to a certain extent. Therefore, these threats should be treated with special care and some of them should be prevented, and some should be mitigated.

As the tendency of modern business is for business entities to exchange data more and more and to create services in the digital economy that increase the quality of life of citizens, the area in cyberspace where it is possible to exploit vulnerabilities is increasing day by day. A large part of that problem is the growing tendency to incorporate IoT devices into critical infrastructure. Therefore, it is important to conduct comprehensive analyzes of how the exploitation of some vulnerabilities affects not only the critical infrastructure subsystem in which it occurs, but also related subsystems. Based on this, it is necessary to create well-designed measures for the prevention and localization of cyber attacks, as well as different recovery scenarios. It is a challenge and a subject for further and more detailed research, to which every country should pay special attention, if it wants the life of its citizens to be safe.

REFERENCES

Albino, V., Berardi, U., & Dangelico, R. M. (2015). Smart Cities: Definitions, Dimensions, Performance, and Initiatives. *Journal of Urban Technology*, *22*, 3–21. https://doi.org/10.1080/10630732.2014.942092

Alladi, T., Chamola, V., & □eadally, S. (2020). Industrial Control Systems: Cyberattack Trends and Countermeasures. *Computer Communications*, *155*, 1–8. https://doi.org/10.1016/j.comcom.2020.03.007

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., Lee, G., Patterson, D. A., Rabkin, A., Stoica, I., & □aharia, M. (2010). A view of cloud computing. *Communications of the ACM*, *53*(4). https://doi.org/https://doi.org/10.1145/1721654.1721672

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, *54*(15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010

Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. *Computer Communications*, *54*, 1–31. https://doi.org/10.1016/j.comcom.2014.09.008

DIVD-2024-00011 - Six vulnerabilities in Enphase IQ Gateway devices, (2024). https://csirt.divd.nl/cases/DIVD-2024-00011/

Candan, B. (2024). *Top 5 critical infrastructure cyberattacks*. https://www.anapaya.net/blog/top-5-criticalinfrastructure-cyberattacks

Clim, A., Toma, A., ota, R. D., & Constantinescu, R. (2023). The Need for Cybersecurity in Industrial Revolution and Smart Cities. *Sensors*, *23*(1). https://doi.org/10.3390/s23010120

Cocchia, A. (2014). Smart and Digital City: A Systematic Literature Review. In Renata Paola Dameri & Camille Rosenthal-Sabroux (Eds.), *Smart City How to Create Public and Economic Value with High Technology in Urban Space* (Progress i, pp. 13–43). Springer International Publishing. https://doi.org/https://doi.org/10.1007/978-3-319-06160-3_2

Das, R., & Gündüz, M. . (2019). Analysis of Cyber-Attacks in IoT-based Critical Infrastructures. *International Journal Of Information Security Science*, *8*(4), 122–133.

Đurđević, M. (2009). *Komunalna infrastruktura* (2. izdanje). Visoka građevinsko-geodetska škola.

García aballos, 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.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660. https://doi.org/https://doi.org/10.1016/j.future.2013.01.010

Hollands, R. G. (2008). Will the real smart city please stand up? Intelligent, progressive or entrepreneurial? *City*, *12*(3), 303–320. https://doi.org/10.1080/13604810802479126

Laković, D. (2025). Cybersecurity Aspects of Critical Infrastructure in Scenario of Smart City. *ALFATECH – Smart Cities and Modern Technologies*, 54–59. https://doi.org/10.46793/ALFATECHproc25.054L

Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing*. https://doi.org/10.6028/NIST.SP.800-145

Milosavljević, B., & Vučinić, D. (2021). Odnos prema kritičnoj infrastrukturi u Republici Srbiji. *Vojno Delo*, *73*(4), 42–56. https://doi.org/10.5937/vojdelo2104042M

Musa, S. (2016). Smart Cities - A Roadmap for Development. *Journal of Telecommunications System & Management*, *5*(3). https://doi.org/10.4172/2167-0919.1000144

NESSI. (2012). *Big Data: A New World of Opportunities, NESSI White Paper*.

NIST. (2022). *critical infrastructure*. Committee on National Security Systems (CNSS) Glossary. https://csrc.nist.gov/glossary/term/critical_infrastructure

Panagiotou, N., ygouras, N., Katakis, I., Gunopulos, D., acheilas, N., Boutsis, I., Kalogeraki, V., Lynch, S., & O'Brien, B. (2016). Intelligent Urban Data Monitoring for Smart Cities. In B. Berendt, B. Bringmann, É. Fromont, G. Garriga, P. Miettinen, N. Tatt, & V. Tresp (Eds.), *ECML PKDD: Joint European Conference on Machine Learning and Knowledge Discovery in Databases* (pp. 177–192). Springer. https://doi.org/10.1007/978-3-319-46131-1_23

Papadokostaki, K., Mastorakis, G., Panagiotakis, S., Mavromoustakis, C. X., Dobre, C., & Mongay Batalla, J. (2017). Handling Big Data in the Era of Internet of Things (IoT). In Constandinos X. Mavromoustakis, George Mastorakis, & Ciprian Dobre (Eds.), *Advances in Mobile Cloud Computing and Big Data in the 5G Era* (1st ed., pp. 3–22). Springer. https://doi.org/10.1007/978-3-319-45145-9

Rieß-Marchive, V. (2023). *Olsztyn, Pologne : quand une cyberattaque fait dérailler la Smart City*. https://www.lemagit.fr/actualites/366543032/OlsztynPologne-premiere-Smart-City-touchee-par-unecyberattaque

Rose, K., Eldridge, S., & Chapin, L. (2015). *The Internet of Things: An Overview - Understanding the Issues and Challenges of a More Connected World*. https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf

Simić, K., Despotović rakić, M., Bojović, Ž., Jovanić, B., & Knežević, Đ. (2016). A platform for a smart learning environment. *Facta Universitatis - Series: Electronics and Energetics*, *29*(3), 407–417. https://doi.org/10.2298/FUEE1603407S

Trbojević, M. (2018). aštita kritičnih infrastruktura - iskustva tranzicionih zemalja. *Politička Revija*, *56*(2), 99–118. https://doi.org/10.22182/pr.5622018.5

Uredba o kriterijumima za identifikaciju kritične infrastrukture i načinu izveštavanja o kritičnoj infrastrukturi Republike Srbije. (2022). *Službeni Glasnik Republike Srbije*, *69*.

Vesić, S. L., & Bjelajac, M. (2023). CYBER SECURITY OF A CRITICAL INFRASTRUCTURE. *Pravo - Teorija I Praksa*, *40*(2), 77–88. https://doi.org/10.5937/ptp2302077V

akon o kritičnoj infrastrukturi. (2018). *Službeni Glasnik Republike Srbije*, *87*.

Žegarac, . (1998). *Infrastruktura*. Geografski fakultet.

Contact information:

Duško Laković, PhD, assistant professor,
1973
Ministry of the Interior of the Republic
of Serbia, Višegradska br.18,24000
Subotica
duskolakovic1@gmail.com
https://orcid.org/ 0000-0001-9984
9669