ALFA BK UNIVERSITY
FACULTY OF INFORMATIONTECHNOLOGY
FACULTY O F MATHEMATICS AND COMPUTER SCIENCE
International Scientific Conference

Alfa BK Univerzitet

UDK:004.8:351.817
711.45:004.78
DOI: 10.46793/ALFATECHproc25.054L
Original scientific paper

Cybersecurity aspects of critical infrastructure in scenario of smart city

Duško LAKOVIĆ

Abstract: People organize their lives and work in a space for which it is important to have adequate infrastructure. Critical infrastructure is the most important part of the infrastructure that has a great impact on the security of the state, its economy and society as a whole. These are interconnected systems, which are part of a larger system, where their functioning relies heavily on the ability of another subsystem to provide the necessary service. The cyber security of such systems is particularly important because such vulnerabilities are singled out and can cause a chain effect that extends from the subsystem to the state. With the development of sensor technologies, the Internet of Things, cloud computing, big data, and artificial intelligence, a range of solutions can benefit business operations. Critical infrastructure companies are not immune to global changes, embodied in the vision of smart cities, which should bring improvement to humanity. On the other hand, introducing "things" into critical infrastructure opens up a whole set of problems that were previously unknown. This paper deals with those aspects.

Keywords: cybersecurity, critical infrastructure, smart city

1 Introduction

From the earliest days, man has adapted the environment to himself with the aim of using natural potentials and resources. In this way, society is created, and the existence of man and community 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. These are systems of clear and clean connections, where all sub-systems are visible, down to the end elements and pronounced vertical connections (Lukić, 2005, p. 5). It is a complex system composed of a large number of other subsystems, which are systems in themselves. That is why it acts as a system of systems, where the business processes of one system rely on the services that the other system offers by executing its business processes. In this context, the role of cooperation between systems is very important, and this includes those services that a subsystem requires from others and those services that one subsystem offers to other subsystems.

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 intentions. 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, critical infrastructure is the most important part of a state's infrastructure, which the state must build, maintain and provide with special care because its failure to function creates a whole set of problems and far-reaching consequences.

Global trends affect the drop in sensor prices and the appearance of a large number of cheap electronic devices, sensors, and microchips that can be installed in some infrastructure elements and provide data on the observed phenomenon. These devices, popularly called "things", use the largest global network - the Internet, to be able to exchange data on the phenomena they observe, and in some cases even act on these phenomena as actuators. They are installed in objects of critical infrastructure and in this way enable the solution of problems that existed in these complex systems, which could not

be solved until that moment with ICT solutions available at that time.

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. Since smart cities rely on the operation of "things" to make city services more efficient, they are under constant threat from such attacks.

The first chapter is introductory. 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 (“Zakon 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 Zaballos & 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 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. In this way, it is possible to support new or improved business models. One important segment is how to integrate this set of technologies with the existing traditional ones, which is supported through the hybrid cloud scenario.

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.

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 water used. In this context, IoT modules take over the functionality of water meter readings, which reduces the need to engage people who until now performed the mentioned processes manually, most often with the use of PDA devices. In this way, all reading errors that occur as a result of manual data entry are eliminated. 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 realization of an important business process of the water company is realized. 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 state.

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 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 destination to destination. 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 consequences for citizens and society as a whole.

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 Olsytyn, Poland, a cyber attack took place on June 24 and 25, 2023, in which the smart systems that regulated traffic were disabled (Rieß-Marchive, 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.

6 Conclusion

Critical infrastructure is the most important part of the total infrastructure. It is characterized by the interconnectedness of systems and is usually defined at the level of one country. At the same time, it refers to the intensive use of information and communication technologies. Smart cities are a vision of a modern society where intensive data exchange and human interaction with technology are realized in order to improve the quality of life. In such an environment, the role of "things" is very significant and they form an important part of the infrastructure elements. Given that "things" use the public Internet, the potential threats coming from the cyber world are very large with numerous related problems if the vulnerabilities of these systems are exploited. Since critical infrastructure subsystems rely on each other, well-designed cyber attacks can disable not only the targeted critical infrastructure subsystem but also those that rely on its services. This can produce cascading effects in which the security of the state is significantly threatened.

On the other hand, critical infrastructure systems largely use operational technology in their operations and at the same time have their own information technologies. Every day, these two technologies are increasingly integrated with each other, and in this way, the surface on which it is possible to carry out a cyber attack is becoming larger and more heterogeneous. As an increasing number of IoT devices are embedded in critical infrastructure, comprehensive measures need to be implemented to protect it in the long term, and where this is not possible, well-thought-out recovery scenarios.

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., & Zeadally, 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., & Zaharia, 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-critical-infrastructure-cyberattacks

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. Z. (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 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.

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

Lukić, B. (2005). *Uloga infrastrukture u prostornom razvoju Srbije: doktorska disertacija*. Geografski fakultet, Univerzitet u Beogradu.

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., Zygouras, N., Katakis, I., Gunopulos, D., Zacheilas, 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/Olsztyn-Pologne-premiere-Smart-City-touchee-par-une-cyberattaque

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 Zrakić, 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). Zaštita 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

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

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

Contact information:

Duško Laković, PhD, assistant professor,

1973

Ministry of the Interior of the Republic of Serbia,

Višegradska 18 Subotica 24000

duskolakovic1@gmail.com

https://orcid.org/ 0000-0001-9984-9669