NAUKA I DRUŠTVO
Časopis za društvene nauke

Beograd,
2021.

NAUKA I DRUŠTVO - Naučni časopis za društvene nauke
(Časopis izlazi dva puta godišnje)

Science and Society – Journal of Social Sciences
(The Journal is published twice a year)

Nauka i društvo izlazi od 1966. godine, a od 2014. godine u formi naučnog časopisa, a od 2018. godine ima produženu numeraciju brojeva.

Izdavači:
- Udruženje „Nauka i društvo Srbije", Beograd, www.naukaidrustvo.org
tel. 011/2456 952, elektronska adresa: nauka_drustvo@yahoo.com
- Studije pri Univerzitetu, Univerzitet u Beogradu

Tehnički urednik i likovna oprema: dipl. ing. Stevan Šormaz

Štampa: Gorapres, Beograd.

Tiraž: 200

CONTENT

Review Paper
UDC: 625.746.5.
DOI: 10.5281/zenodo.5525156
Received: 2 March 2021
Accepted: 12 March 2021

Ilija ŽIVOTIĆ*

Faculty for Engineering Management – FIM, Belgrade

Ratomir ANTONOVIĆ

Faculty of Law, Security and Management „Constantine the Great“ Niš
Union Nikola Tesla University, Belgrade.

MANAGEMENT SECURITY CRISIS ARISED TRAFFIC IN THE PROCESS OF ABUSE OF TRAFFIC LIGHTS

Abstract

Traffic light signalization is nowadays one of the most reliable means for regulating public traffic in all major cities in the world. Relying on traffic police officers who regulate traffic at intersections or respecting the so-called the rules on the right represent long-forgotten methods of regulating traffic. Traffic lights are part of the so-called smart systems that have their own electronic systems that control their operation. Therefore, the traffic light can be the target of cyber-attacks, all in order to create traffic problems, which result in congestion of large city streets, which can be a suitable terrain for committing certain terrorist acts, as well as other crimes. Therefore, in this paper, the traffic light is considered not only as a device for regulating traffic, but also as a means suitable for manipulation and abuse by criminal and terrorist organizations.

Keywords: *traffic, signalization, cyber-attacks, sabotage, terrorism*

* representative@ilijazivotic.com

INTRODUCTION

Traffic light signaling and intelligent traffic signaling systems are undoubtedly an important component in the evolution of the so-called smart cities. They are important in the process of planning and regulating traffic and traffic jams, which are becoming one of the biggest problems in the functioning of almost all world metropolis. These complex traffic systems include first vehicles, then lights signaling, sensors and traffic infrastructure. In order to overcome the growing traffic problems, modern cities are developing efficient innovative applications of intelligent signaling systems with the task of directing and regulating traffic jams. Optimal traffic control, raising traffic safety, regulating traffic at major intersections, as well as raising the quality of emergency reporting, in terms of traffic collapses or accidents, are imperative tasks of modern signaling, surveillance and monitoring systems for public traffic in large cities.

In this procedure, traffic lights have the most important role. The coordination of traffic lights and their harmonization enable a good flow of vehicles, unnecessary stopping and slowing down of movement are reduced, and the circulation of vehicles itself and other traffic participants is of better quality and more fluid. Traffic light signaling and electronic traffic regulation in cities works according to the principles of hardware, which are specially made for these needs. They enable accurate and precise regulation of vehicle movement, while respecting certain principles that first guarantee safety for all traffic participants. On the other hand, these systems are vulnerable to cyber-attacks. Specifically, the hardware of these devices can be subject of cyber-attacks and sabotage, which could result in destabilization of traffic safety on one or more roads in the city.

Attacks on traffic lights could first contribute to shifts from factory to inaccurate settings, traffic lights could be permanently disabled for work or provide inaccurate information to traffic participants. Information technology experts point out that the sabotage of traffic lights and signaling devices from nowadays aspect is not a very complex and demanding undertaking. These systems can be influenced relatively easily and without major material

investments. Although these types of attacks are not frequent and for now we can talk more about them from the aspect of theory, the fact is that the safety of light and traffic lights system should be discussed in a little more detail and analyzed, especially if we take into account that the Road Safety Strategy of measure development of any country can be seen through the level of achieved development of the traffic system.

To that end, it is necessary to assess the risk of attacks on traffic lights and light signaling as an effective means of assessing the security implications of the vulnerability of these systems, with proposals for defensive measures against potential attacks. The competent bodies of the traffic police, as well as experts in the field of synchronization and installation of traffic lights and light signaling must participate in making the assessment. They must be in constant readiness from cyber-attacks on these devices, with the present awareness of the possible consequence if the attack itself occurs. Also, a good theoretical framework is needed, through which all possibilities of cyber-attack on traffic lights and other signaling devices would be processed, with starting points on the importance and necessity of traffic light and other light signaling in traffic regulation in large cities, the fact that these electronic systems for traffic regulation are vulnerable and may be a potential target of terrorist attacks and other persons aimed at destabilizing traffic safety, with the aim of maximally optimizing cybernetic traffic safety and recognizing the priority of defensive measures to mitigate the risk of cyber-attacks on signaling devices.

FUNCTIONING OF TRAFFIC SIGNALS

In large cities, where the traffic frequency is expressed, the traffic is regulated with the help of traffic lights and light signaling. Signals at intersections are coordinated by light systems, which function according to certain principles. Adjustments of these systems are made through the harmonization of traffic cycles, which are adjusted by phases, their order and duration. Traffic light signaling is synchronized in repeated cycles, and the cycles consist of several sequential phases. For example, it is necessary to synchronize a longer phase in those traffic directions where a weaker flow is expected, because this helps to encourage it, while proper shifting of cycles and sequence of phases is needed

when trying to shorten the waiting time for departure at intersections. During this synchronization, special attention must be paid to all permitted directions of movement at the intersection, and each phase must refer to certain movements in certain directions.

Traffic light signaling determines the waiting time at the intersection directly, that is, indirectly affects the traffic density and its flow. Traffic light signaling must be understandable to every traffic participant, it must be accessible and it must enable good communication of all traffic participants. Traffic light signaling is a significant factor when calculating the route, as well as the speed of reaching the destination, which is calculated by GPS devices. Good synchroni- zation of these devices enables more accurate calculation of the required time interval to reach the destination, with less deviation.

In relatively light traffic systems, which are characterized by lower traffic frequency, each available route is equally acceptable to traffic participants and whichever one they choose, it needs the same or similar time interval to arrive at the destination location. In contrast to this situation, the behavior of traffic participants must be absolutely different in traffic systems that are congested and overloaded. The choice of a bad route leads to traffic jams, congestion of certain roads and to the non-functionality of the traffic system in the city. In such systems, it is best to choose the routes of movement in fragments and, if possible, on the basis of estimates that refer to the gradual easing of the frequency of the given roads.

As a significantly aggravating factor in the regulation of traffic in large cities with the help of traffic lights and other modern devices, there is an interdependence of all significant traffic routes, which are intertwined, connected and dependent. The burden of one significant direction therefore means the burden of other directions, which are in a mutual relationship of dependence. According to some ideal ideas in theory, in such situations the existence of a system of special observation of the traffic network in the city would lead to the existence of an advisory device in each vehicle, which would suggest to drivers which route to choose at a given moment to avoid traffic jams and congestion of given roads. Ideally, all drivers should follow the given instructions and follow the recommended routes, which would lead to maximum compliance with the given time intervals for arriving at the

destination location and enable optimal traffic flow. The system of advice to drivers would be provided by a system of monitoring the movement of all vehicles, and would be notified of any deviation from the route and would arrive as a notification to other traffic participants, to plan potentially new routes or to calculate a new time interval for arriving at the destination.

In addition to intersections where traffic is evenly distributed along the routes, in almost all areas there are a number of intersections where one direction (street) is significantly more congested than the other direction. For such intersections, it is necessary to develop digital hardware that enables the maximum flow of vehicles in the direction that is more loaded with vehicles. The basic requirement that such a digital device should meet is to allow a minimum duration of the permitted passage (green light) on the main street of 25 s and to maintain such a state until the vehicle arrives on a side street. The arrival of vehicles in a side street initiates a change in the situation at the traffic lights, so that the arrival of arrived vehicles is enabled. The duration of the allowed passage in the side street is until the passage of all vehicles coming from the side street, and for a maximum of 25 s. This means that during the continuous arrival of the vehicle from the side street, the traffic light works in the normal mode, with the same duration of the state „allowed passage“ and „stop“ on the main and side street. Between the „allowed passage” and „stop” states there is a „warning” state (yellow light on the traffic light) that lasts 4 s.

SECURITY ASPECTS OF TRAFFIC LIGHT SIGNALING ABUSE

In order to be able to analyze in detail the possible safety endangerment to traffic through the misuse of traffic lights and other signalization, it must first be explained from a technical point of view only the functioning of traffic lights as a device. The traffic light consists of: 1) controllers, which regulate light conditions, 2) sensors, which detect traffic conditions, 3) unit for managing possible system errors.

Controllers have a particularly important role for the functioning of traffic lights, because they directly condition the changes of light signals, which

directly affects the functioning of traffic. As a rule, a certain light signal (red, yellow and green pain) lasts as long as it is programmed, in precise time intervals. In addition to standard signals, there may be semi-activations or directions that must always be included, such as an indicator of a conditional passage through an intersection, popularly known as a „green arrow“. The controllers receive information from sensors, which activate the states of change of light signs in the optimal and pre-programmed time interval.

The controllers are physically located near the intersection and traffic lights in special metal cabinets, which are kept locked. These cabinets contain controllers with sensors, which send information about changes in light signals on traffic light devices. It clearly follows from the above that this type of storage of controllers and sensors does not belong to the category of the most efficient. Especially since the cabinets can be easily opened and their contents accessed without authorization. It logically follows that persons who have adequate technical knowledge and skills can influence the operation of traffic lights directly and traffic safety indirectly. If this type of sabotage were carried out continuously at a larger number of intersections in the city, which are in a relationship of interdependence, it is clear that a larger security problem could be caused.

The most sensitive and primarily targeted by potential attackers would be controllers, because they could be used to influence changes in light signals at traffic lights. The attack is carried out by denial the service to the operating systems, which in turn reflects on the change of light signals at the intersection, bringing traffic safety into question and in a state of endangerment. The influence of these attackers is primarily manifested on the commands for adjusting the light lamps on the traffic light device.

The essence of the attack is the negative impact on the control process and the rhythmic change of light signals at the traffic light. Sending incorrect information to the controller leads to a longer delay of the vehicle, by keeping the red light for example or a situation where all traffic participants would be allowed to pass at the same time, which would undoubtedly lead to traffic accidents at that intersection. This situation is in direct opposition with a goal number 1 within the framework of the first Pillar of the Traffic Safety Action Plan. In such conditions, the controller works with incorrect

information and sends incorrect commands in changing the light signals, and the sensors function as part of a modified system adapted to the needs of the attacker. The attacker made a backup engineering of the software protocol and used all the problems during the authentication in the network, so that the modified software would react to the information it received from the sensor.

Traffic light systems can also be the target of physical attacks. Then the hardware of these devices is directly endangered. Damage and disabling of hardware in light signaling systems leads to the configuration of dangerous light and signal conditions, which can cause the extinguishing of certain light signals, their too short or too long emission or simultaneous emission of the same light signals to all traffic participants, which inevitably leads to crisis situations.

SECURITY RISKS OF TRAFFIC LIGHT ABUSE

It is an indisputable fact that traffic light systems are an easily vulnerable category. The reason for that is, as already mentioned, first of all in the easy accessibility of the systems of these devices, which are mostly located at intersections, or their immediate vicinity, without adequate protection. Also, it was stated that the systems that directly affect the operation of traffic lights at intersections are easy to read for those who know the technique, and that their work can be influenced without major difficulties. Any influence that is not from the competent services can be very dangerous for traffic safety and traffic participants.

In order to prevent such safety risk situations, it is necessary to perform a safety assessment, which is the basis for considering the safety position of these light signaling devices. Also, it is necessary to build awareness of the danger of negative impacts on traffic light signaling at those bodies that deal with traffic safety, and that among the priority issues is the issue of traffic light safety and their protection from potential attacks. At the moment, it is very difficult to predict all the modalities of possible attacks on traffic lights in all developed cities in the world. The possibilities are really great and the attackers have a wide range of mechanisms of influence on these devices, their

disabling and putting into function of a terrorist attack or some other harmful and dangerous event. In order to be able to answer the question about the possible modality of the attack in detail, it is necessary to do a detailed analysis of all sources of attacks, as well as to realistically look at the vulnerabilities and weaknesses of these systems.

Any unwanted situation, which is the result of traffic light obstruction, can be defined as a degradation of traffic management performance. It can be the result of an attack on traffic light signaling, and the harmful consequences of that attack can be manifested through negative results, such as congested and impassable roads, the longer time required to reach the destination location, frequent traffic accidents and the like.

When assessing the security risks of misuse of traffic light signaling and attacks on these systems, the consequences that occur under different circumstances must be differentiated with maximum anticipation of potentially worst consequences, which is in line with the horizontal framework of the European Critical Infrastructure Protection Program. Also, it is necessary to anticipate potential events that may occur as a result of the attacker's actions, with anticipation and the effects they want to achieve through the realization of the attack itself. The attackers act by trying to discredit the existing traffic light and signaling system, by modifying that system and changing the rhythm of the light signals that are emitted. This inevitably worsens the performance of traffic management on the one hand and affects the behavior of traffic participants on the other hand, which has the ultimate effect of redirecting traffic to a certain side. It is logical to conclude that the attacker's goal is to group as many vehicles and traffic participants in one place, which is, for example, the subject of a terrorist attack, because the mass of victims is one of the most important features of terrorism and terrorist acts.

Also, the problem of traffic destabilization through traffic light obstruction and light signaling can be observed from the aspect of the already mentioned GPS system and navigation system, which calculates the shortest and fastest route to the destination location for the needs of the driver. When entering driver preferences, in terms of destination location, the system calculates the shortest and fastest route, giving an optimal time frame. In the calculation of the time frame, the essential component consists of traffic lights and retention

on them, which can be determined with greater or lesser precision by mathematical operations. Traffic light obstruction automatically means extending this time frame, forcing participants to abruptly and unplanned route changes, all of which can result in congestion of certain road routes and reduced traffic safety for traffic participants.

MECHANISMS FOR SOLVING TRAFFIC SIGNAL SAFETY PROBLEMS

The problem of traffic safety, which can be violated through the negative impact on the operation of traffic lights and traffic signaling must be approached from the aspect of complex consideration and solution. The complexity of traffic as a system, composed of several elements, must be taken into account, with all the unpredictability of traffic participants and the existence of situations that can be characterized as risky.

In order to ensure a minimum of traffic safety, in the process of making and designing traffic systems, special attention must be paid to the safety moment. Manufacturers of traffic lights and other signaling devices must also keep in mind the possibility of cyber-attacks on these devices and the impact on their safe operation when making them. There are essential changes in the design of the controller in order to aggravate and disable unauthorized access, as well as disabling unauthorized influence on the debug port, which is otherwise very suitable for affecting the device system memory, as well as the ability to reconfigure the system.

One of the very common oversight is leaving factory codes on the devices. Manufacturers generally enter the same factory codes into all systems, and it happens that all traffic lights in the city have the same code. By detecting the code at one traffic light, the codes were detected at all the others, which significantly facilitates the position of the attackers and gives unimagined possibilities. It is recommended that the codes are changed regularly, that they are not left at the factory settings, but that each traffic light has its own authentic codes, as well as that these codes are reset and changed at a certain time interval.

At the same time, network communication within these signaling systems

must be encrypted, which would provide more efficient and secure exchange of information and data. The dangers of unauthorized access to the system of communication, eavesdropping and retrieval of information between two or more controllers would be eliminated. Sensor software must be designed so that any arbitrary and unauthorized change is impossible. Also, the communication system between the sensor and the controller must be time-marked, which in practice means the impossibility of repeated attacks and sending already sent information.

In theory, there are advocates who do not support the application of these measures of protection the safety and efficiency of traffic light and signal devices. There are theories that indicate the obligation to level these safety measures with the needs of traffic, with the specification of priorities and the application of combined measures for traffic safety and traffic signaling. Adequate security measures can minimize all weaknesses in these signaling systems and devices.

In the application and implementation of traffic safety measures and traffic lights and signaling devices, there are three active participants: traffic management body, attackers and traffic participants.

The traffic management authority applies security measures to ensure signal and traffic light devices at intersections in cities, with maximum reduction of the potential for a possible attack. Attackers easily overcome the obstacles of insufficiently protected traffic light and signal devices, subordinating them to their needs and ideas, all with the aim of destabilizing traffic and introducing insecurity. Traffic participants, driving their motor vehicles, are constantly searching for the most passable and fastest routes to their final destinations.

The interests of traffic management authorities and traffic participants are compatible. Attackers have opposing interests, and it can be said that the body and participants must act in a coordinated manner in order to thwart the attacker's intentions, because the realization of the attacker's intentions endangers the interests of traffic management bodies and traffic participants. While attackers look for system weaknesses, the traffic management body and traffic participants must minimize these weaknesses and act compactly in implementing measures that raise traffic safety to a higher level.

The problem of the vulnerability of traffic lights and traffic light signaling in traffic was pointed out in 2013 by the US Department of Homeland Security in the Critical Infrastructure Protection Plan. Traffic lights and signaling lights which is used to regulate traffic are classified as critical infrastructure, which has become an important and essential part of national security, and its protection is one of the priorities of every country. On that occasion, all potential modalities of the possibility of endangering the safety of traffic signals were theoretically elaborated, with special reference to cyber-attacks and sabotage of traffic lights. At the same time, the key problems of traffic safety and the weakest points in the work of traffic lights and signalization were marked. These are the already mentioned problems of obsolete factory codes and the openness of the debug port.

That the protection of traffic lights and other signalization is necessary is already indicated by some successful attempts at attack. This primarily refers to a relatively cheap and easily accessible device, which enables wireless sensor change of light signals on the traffic light, whose creator is Cerrudo. Another example of an attack and disabling of a traffic light was noted when changing the time configuration of the controller, which is most often divided into working and weekend days as well as summer-winter periods, which directly jeopardized the traffic light mode.

The focus of the research on the vulnerability of traffic light signalization is the assessment of the safety and resistance of traffic systems, which especially includes optimal control and preparedness for a potential cyber-attack. Of particular importance are the components for monitoring and control, as well as the permanent analysis of the existing network performance and its resistance to potential attacks. The goal of the research is to determine the vulnerability of traffic systems in the conditions of unauthorized cyber-attacks, which have the task of disabling those systems and subordinating them to their needs and the realization of their plans. At the same time, in addition to cyber-attacks, the analysis should provide an answer to how these systems would react in the conditions of natural disasters and whether they would be resistant to that type of influence, which does not come from humans, but from some higher force.

Also of great importance is the analysis of the work of traffic lights, which are

related to the work of ramps, which control the possibility of traffic flow. The system of measuring the time for the openness, ie the closure of the ramp, is based on the techniques of optimal traffic management in optimal conditions. Disruption of ramp operation metrics clearly endangers traffic safety, because enabling the crossing in conditions when it is not safe, directly endangers all traffic participants.

CONCLUSION

In a period when terrorist activities are in significant expansion, special attention must be paid to every possible form of terrorist act. Through the process of analyzing the risk of terrorism and terrorist attacks, all potential weaknesses of the different systems that may be the target of attacks must be highlighted.

Traffic is generally has great security potential due to the whole set of circumstances that mark it as high-risk. Motor vehicles themselves, their use, movement and the performance they have, represent a sufficiently clear safety risk. This is supported by data on more frequent and more intensive traffic accidents with a big fatal outcome, as well as big consequences for the lives and health of people, participants in traffic.

Traffic infrastructure, its maintenance and renewal, also have a strong security risk. Bad traffic infrastructure is often the cause of traffic accidents, and old and insufficiently well-maintained roads, poorly marked and visible roads must be mentioned as a problem, especially when driving in difficult traffic conditions, such as fog, rain, snow or in the dark. The problem of removing traffic signs, their theft and destruction should be mentioned here, which greatly endangers traffic safety and makes it difficult for traffic participants to drive motor vehicles.

Traffic and traffic light signaling have a particularly important place in the work, and they are observed from the aspect of their technical-technological equipment, their performance and work model, as well as from the aspect of their potential to endanger traffic safety. Although designed to be the most important trump card in regulating traffic and raising traffic safety, by malicious use and influencing the regime of their work, they are becoming a

powerful weapon in the hands of terrorists and attackers. The paper itself points out the weaknesses of these traffic light systems, and clearly marks the weaknesses in their work and points to the potential possibility of their abuse.

Raising the security of these devices can be achieved at the technical-technological level, which is a priority task of manufacturers of traffic lights and other signaling equipment, raising security protection of these devices, as well as disabling potential any unauthorized access that would disrupt factory set work process. Better protection of these devices can be achieved by full digitalization of traffic lights, based on wireless communication in traffic light components from the central system, which would not be easily accessible and visible.

The current situation in all large cities, where traffic light systems exist, does not meet the minimum-security criteria in the least, and these systems can be characterized as easily vulnerable and suitable for a possible attack. The paper itself points out the vulnerabilities of this system and gives certain suggestions in order to raise security to a higher level. There is a special emphasis on the problem of factory-determined codes that are universal for all traffic light systems, the problem of their easy understanding, which then opens up the possi- bility of influencing the entire system.

Also, the paper points out all the potential consequences of such cyber and terrorist attacks on traffic lights and signalization in large cities. The entire behavior of all traffic participants is subjected to changes if the manipulation of traffic lights is successfully carried out. This can result in congestion of important city roads, endangering the safety of traffic participants and creating a suitable situation for the execution of some activities that could endanger the lives and health of a large number of people.

REFERENCES AND SOURCES USED

Albert, Reka; Jeong, Hawoong,Barbasi Albert, Laszlo, ,,Error and attack tolerance of complex networks" Nature, No.406, 2000.

Cerrudo, Dharani, Yunpeng, Zhang, Liang, Cheih, Cheng: ,,Hacking US traffic control systems", available at: https://www.defcon. org/images/ def-con-22. 01.12.2020

Danković, Danijel; Sinadinović, Vladica; Milosević, Dusan; Prijić, Zoran. „Realizacija Inteligentnog semafora, na bazi Nanoboard-a 3000", Indus- trijska elektrotehnika INDEL ,2010, Electrotehnical Faculty , University of Banja Luka,(Branko Dokić), Banja Luka,2010

European Union; EU Commission of the European Communities. ,,European Programme for Critical Infrastructure Protection", Brussels, 2006

Grubor, Gojko; Milosavljević, Milan. „Osnove zaštite informacija, metodološko-tehnološke osnove", Singidunum University,Belgrade, 2010.

Komanduri, Saranga, Shay, Richard, Kelley, Gage, Patrick, Mazurek, Michaelle, Bauer, Lujo, Christian, Nicolas, Cranor, Faith, Lorrie, Egelman, Serge: 'Of passwords and people: measuring the effect of password-com- position policies'. Proc. SIGCHI Conf. Human Factors in Computing Sys- tems, Association for Computing Machinery, New York, 2011.

Laszka, A., Potteiger, B., Vorobeychik Yevgeniu., Amin, Saur- bh, Koutskouts, Xenofon.: 'Vulnerability of transportation networks to traffic-signal tampering'. Seventh Int. Conf. Cyber-Physical Systems (IC- CPS), 2016 ACM/IEEE,(editor Bradley Schmeri), Vienna, 2016

Li, Zing, Jing, Dong; Hannon, Christopher; Shahidehpour, Mohammad; Wang, Jianhui. „Assessing and mitigating cybersecurity risks of traffic light systems in smart cities", IET Journals, Vol. 1, Iss. 1, 2016.

Ministry of Construction, Traffic and Infrastructure of the Republic of Serbia (2015). „Road Traffic Safety Strategy", Belgrade.

Ozier, O. (1999). „Risk Analysis and Assessment, Handbook of Information Security Management“, CRC Press, Boca Raton, Florida.

Radovanović, A., Ristović, M. (2015). „Upravljanje saobracajem na slozenoj raskrsnici koriscenjem sistemskih funkcija PLK Simens S7-300 ” book of papers INFOTEH - Jahorina Vol.14 (Slobodan Milojkovic), University in East Sarajevo, Electrotechnical Faculty, pp 886.

Skero, M., Ateljević, V. (2015). „Zaštita kritične infrastrukture i osnovni elementi usklađivanja sa direktivom Saveta Evrope”, Vojno Delo 3/2015, Belgrade, p.192.

Government of Republic of Serbia (2017). „Action Plan for the Implementation of the Traffic Safety Strategy”, Sluzbeni Glasnik 1/17, Belgrade.

Илија ЖИВОТИЋ

Факултет за инжењерски менаџмент ФИМ, Београд

Ратомир АНТОНОВИЋ

Правни факултет, безбедност и менаџмент „Константин Велики“, Ниш
Универзитет Никола Тесла, Београд

УПРАВЉАЊЕ БЕЗБЕДНОСНОМ КРИЗОМ РЕГУЛИШУЋИ САОБРАЋАЈ У ПРОЦЕСУ ЗЛОУПОТРЕБЕ САОБРАЋАЈНИХ СВЕТАЛА

Апстракт

Семафорска сигнализација данас је једно од најпоузданијих средстава за регулисање јавног саобраћаја у свим већим градовима света. Ослањање на саобраћајне полицајце који регулишу саобраћај на раскрсницама или поштујући такозвана правила десне стране представљају давно заборављене методе регулисања саобраћаја. Семафори су део електронских система којима се контролише саобрачај. Стога семафор може бити мета сајбер напада, а све у циљу стварања саобраћајних проблема, који резултирају загушењем великих градских улица, које могу бити погодан терен за вршење одређених терористичких аката, као и других кривичних дела. Стога се у овом раду семафор не сматра само уређајем за регулисање саобраћаја, већ и средством погодним за манипулацију и злостављање од стране криминалних и терористичких организација.

Кључне речи: *семафор, сигнализација, саботажа, сајбер напад тероризам*

Research Paper
Paper UDC: 351.741.
DOI: 10.5281/zenodo.5525152
Received: 17 April 2021.
Accepted: 23 April 2021.

Ana VUKOVIĆ*

Institute of Social Sciences, Belgrade

A ONE VIEW ON WORK ETHIC AND POLICE INTERNAL CONTROL**

Abstract

The paper deals with the analysis of the relationship between work ethic and police internal control. In the first part of the paper, we give a brief overview of the concept work ethic in correlation with the characteristics of police profession and organization. The second part of the paper includes an analysis of the relationship between work ethic and internal control in police. The basic thesis is that the efficiency of work (police) ethics reduces the need for internal control. The aim of this paper is to point out that work ethic is conditioned by the application of rules and Code of Ethics. The author concludes that the internalization of ethical principles, as well as the perception of punishing illicit and unethical behavior, creates work and social environment in which ethics is not understood as pressure but as a duty of an individual, social group and organization.

Keywords: *work ethic, police ethics, internal control, police profession, society*

---

*annvukovic@yahoo.com

**This paper was written as part of the 2021 Research Program of the Institute of Social Sciences with the support of the Ministry of Education, Science and Technological Development of the Republic of Serbia