UDC 351.78:355.45(100)

GENERAL ACTIVITIES OF OPPOSING AND PROTECTING AGAINST SECURITY THREATS

Nebojša Bojanić[1]
Faculty of Criminal Justice and Security Studies, University of Sarajevo

Edita Hasković[2]
Faculty of Criminal Justice and Security Studies, University of Sarajevo

Abstract: Security, as one of the fundamental values of social functioning and a key subjective feeling of individuals within a society, is often the target of various attacks. The feeling of insecurity can lead to the internal erosion of society and constant demands to the relevant social control authorities to elevate security measures. However, overly conspicuous actions and clearly visible measures can also undermine the feeling of security, causing people to feel unsafe due to the omnipresence of high-tech cameras, notifications, and law enforcement presence. This may indicateto individuals that something is "not right." The authors of this paper have presented specific preventive-repressive steps and measures in the field of protection against threats. The primary requirement of the security system is deterrence from attacks, which is the aim of preventive measures discussed in this paper. By integrating all forms and types of protection, the degree of threat is reduced, and the level of security is increased. Therefore, this paper presents elements of preventive reaction, with a projection of integrating all subjects in preventing and eliminating security threats in terms of maintaining everyday habitual activities. All the aforementioned is accompanied by a discussion with arguments for and against certain measures, potential encroachments on human rights, and the paper concludes with considerations and proposals for the most effective actions.

Keywords: threats, security, measures, projects, protection

Introduction

The everyday life of a modern individual, as well as society and social systems, is filled with a spectrum of information about various forms of security threats. Security is most often a subjective feeling of an individual, and frequently also of social groups. Through mass media, we very often or daily witness information or news related to security threats or depictions of a state of general insecurity, specifically the presence of various forms of threats to stable political-economic relations and thereby security itself. Security, in the broadest sense, implies the absence of potential and actual dangers for individuals and society (Abazović, 2002). Threats to security are carried out by threatening to attack the life or body of a person or in such a way that causes public unrest. Endangering security is

[1] Contact address: nbojanic@fkn.unsa.ba

[2] Contact address: ehaskovic@fkn.unsa.ba

incriminated in national criminal laws, with its basic and more severe forms. The more severe form of this act involves endangering the security of multiple persons with a serious threat to attack their lives or organs, thereby causing public unrest. Given the aforementioned, the goal of every individual and the community is to achieve the highest possible degree of security, which is achieved through the creation and implementation of adequate security policies. On one hand, the actors of the security system are the state with its law enforcement agencies and judicial system, and on the other hand, individuals and the private security sector, within their jurisdiction. Therefore, the importance of this paper lies in presenting measures and activities to prevent security threats. From the above, it follows that the goal is preventive repressive measures and actions that will prevent security threats or, if security is endangered, reduce the damage or consequences to a minimum.

The subject of this paper is the requirements that need to be met using physical or technical protection measures and actions, which would prevent security threats, while from the subject arises the problem of the work, which is the already visible endangerment of security. The methods to be applied in the preparation of this article are theoretical consideration of the problem through content analysis and methods of deduction and induction from general to specific. The justification for this type of paper lies in the use of means and methods of physical and technical protection primarily through prevention, and in certain situations, also repressive measures.

Preventive Repressive Measures and Actions to Prevent Security Threats

Every protection system, whether physical or technical, aims to reduce the risk of endangerment and increase the chance of discovering and identifying the attackers. According to Duvnjak (2004), there are certain criteria that apply to all subjects in the system of securing objects, especially companies. These are measures that must be proportionate to the risk and have a preventive character, as well as necessary interagency cooperation and cooperation with other security system structures. In addition, it is necessary to understand that security tasks are incompatible with other tasks, and that the quality of the security service is more important than the number of guards. Citizens often, for subjective or objective reasons, seek a higher level of protection than the chance of discovering and identifying the attackers.(Skakavac, 2011). Many agencies are focused on combating and preventing criminal[3] activities and providing protection from offenses directed against public order and peace[4], as well as offering private security services in the domestic market (Mršić, Radić, 2023). According to research by Born, Caparini, and Cola (2007), Kešetović and Davidović (2009), and Storm and colleagues (2010), there is a constant increase in investment and profit in the security sector, confirmed by recent results from 2022 indicating that the

[3] Criminal activities are understood as criminal offenses according to criminal laws. (Criminal Code of the Federation of Bosnia and Herzegovina, Criminal Code of the Republic of Srpska, Criminal Code of the Brčko District of Bosnia and Herzegovina, and the Criminal Code of Bosnia and Herzegovina – sources listed in the literature.

[4] Laws on offenses against public order and peace of the Sarajevo Canton. Official Gazette of the Sarajevo Canton numbers 18/2007, 7/2008, 34/2020, and the Law on Offenses of the Federation of Bosnia and Herzegovina, Official Gazette of the Federation of Bosnia and Herzegovina numbers 63/2014, 41/2022, 68/2022).

security industry is experiencing a significant rise, from manufacturers to service providers (A&S Adria). In this sense, it is accurate to state that investing in security is not an expense but an investment.

Security service personnel or agencies providing security or protection services must particularly take care of self-protection while performing their duties. A company's security system is as strong as its weakest point. Well-designed implementation of security measures and equipment enhances the protection system. This system is connected and supplemented with preventive measures and physical security and is always ready to respond to potential attacks or threats. In practice, several physical security systems are used, such as (Duvnjak, 2004): utilizing the services of specialized agencies for providing physical and technical protection, organizing an in-house security service, organizing a joint security service for multiple companies located in the same building or in close proximity.

According to Ostojić and Knežević (2003), the factors and subjects that can be potential triggers for activating the security system are: people, animals, vehicles, and fire. The primary task of the security system is deterrence from attacks, meaning prevention. The desired goals to be achieved by applying a particular physical or technical protection system against threats include the requirements that a specific system needs to meet. These requirements can be:

a) deterring the perpetrator;
b) early detection of the perpetrator;
c) alarming the perpetrator and intervention teams;
d) slowing down the perpetrator;
e) intervention by physical security or intervention teams;
f) identification of the perpetrator.

Deterring the perpetrator often leads to abandoning the commission of a crime, which is achieved to the greatest extent through the application of integrated anti-burglary subsystems, access control, and video surveillance.[5] By abandoning the criminal act at the very beginning, the requirement for early detection of the perpetrator is met through centralized anti-burglary and access control systems. Activating integrated anti-burglary, fire alarm, access control, and video surveillance systems alarms the perpetrator and intervention teams, allowing to the reduction in the time of the attack on the object or property. The perpetrator, when threatening an object, should encounter systems that will slow him down in his unlawful activities, thereby influencing him to abandon the commission of the crime, enabled by efficient passage and access control. Finally, the awareness that there is a possibility of digital recording of the object, space, or some event of security significance induces fear of the possibility of detection and imposition of criminal sanctions for the committed crime. In other words, it induces fear or apprehension in the potential perpetrator that he will be identified and recognized, and that his act will be attributed

[5] For example, as Korajlić et al. (2012) state, video cameras installed to facilitate the observation of certain locations are increasingly used for population surveillance. Specifically, these systems are being extensively used in the United Kingdom and are referred to as technologically supported physical surveillance. The purpose of the cameras is to assist in the detection, investigation, and prevention of crime. How much these systems represent a violation of individual rights is a matter for discussion; however, in the 21st century, privacy, as the author further notes, can be considered a thing of the past.

to him, with the recording used as material evidence. The recording can only be used as material evidence if the entire procedure of its use is respected from a legal standpoint.

Integrating all forms and types of protection reduces the level of threat to all objects and increases the level of security. This should especially apply to larger objects. The threat pertains to both material goods and human lives, particularly in today's time where the risk to life and general insecurity is increased with the growing number of terrorist attacks and other forms of violent crime. Besides material goods, objects, and valuable items, the threat also pertains to the lives of citizens, employees, service users, visitors, students, casual passersby, etc. The ideal reaction to prevent threats is a combination of physical and technical protection and their integration and centralization. Only in this way the effects of protecting people and property can be increased. When it comes to serious criminal acts, besides the role of agencies for the protection of persons and property, the main role is still played by the police. As Savić (2013) notes, regarding the role of the police in combating, for example, terrorism and other forms of crime, cooperation with the public and gaining its support is of crucial importance. This support cannot be gained by force but by serving the community. This brings to the forefront a strategy of effective and legitimate police action using less violent methods in solving security problems. Ensuring effective protection while not alienating the population being protected is the greatest challenge that needs to be addressed.

Elements of Designing Protection Systems to Reduce Vulnerability

When designing protection systems, it is essential to consider objective elements. Often, only subjective elements are taken into account during the design process. Therefore, modeling should be conducted to enable high-quality design and implementation of object protection. This involves performing various calculations through algorithms for the protection model of a specific object. Objective modeling of the attack concept involves creating a mathematical model of the protected object that describes construction, detection, and blocking elements, their spatial arrangement, and relational interdependencies. Additionally, the assessment model of vulnerability needs to account for the response time of the security service to an alarm or other attack notifications (Čakija, 2011). In this regard, when planning physical security, Duvnjak (2004) states that it is necessary to plan for four to five guards for a 24-hour security post, seven days a week, or 1.5 guards for an eight-hour shift. This is because, for particularly vulnerable objects, the working hours at the guard post need to be minimized to maintain a high level of concentration, which requires more personnel and more frequent changes at the guard post.

Perpetrators are hesitant to attack an object without prior planning. The most common ways of attacking or breaking into objects are: breaking window shutters, entering from upper or lower floors, accessing through gas pipes, gutters, or ventilation systems, unauthorized or forced entry through garages, attacks on entry doors, and ambushes. Given the elements and methods of attack on an object, as well as the time component of the attack duration, alarm response, and other forms of protection, including the response time of the responsible security agency, it is necessary to design and implement an object protection system. To create a protection project for an object, analyses must be performed, which involves considering the following (IDEA, 2016):

a) External analysis of the object, assessing the potential use of gas pipes, gutters, neighboring balconies, and windows for entry into the property;

b) Evaluation of the lighting conditions around the object, as darker areas may facilitate an attack;

c) Clear and decisive analysis of the level of defensive capabilities on the outside of the object, such as wooden, plastic, or aluminum shutters, which are inadequate protection against attacks, while robust iron bars and metal shutters provide more effective protection;

d) Assessment of the presence of people in the protected and neighboring objects: perpetrators will attempt to break in when the number of people who can see or hear unusual noise is minimized;

e) Assessment of the object's defense level relative to neighboring objects, where it is evident that if there are three similar objects on the same floor, two equipped with anti-burglary doors and one not, the latter will be a more attractive target;

f) Assessment of previous theft methods in the area where the object is located; g) Assessment of dynamic situations such as the placement of temporary scaffolding that could facilitate climbing by perpetrators.

In addition to the above, it is necessary to conduct risk analyses to determine the effects and consequences of interruptions or significant disturbances in the operation of objects, especially those marked as critical infrastructure (Sabljić, 2022).

Modern protection systems for larger objects and areas require the installation of perimeter fencing with built-in sensors. The perimeter fencing is also combined with physical barriers, sensors, numerous visible and invisible video cameras, and anti-burglary doors and windows on the object itself.

Thanks to video surveillance, there is a higher probability that the perpetrators of attacks on financial institutions and stores or participants in traffic, at border crossing or some public facilities will be recorded by the video surveillance systems. In practice, video surveillance cameras of varying resolutions and capabilities are used. Practically, it is better to invest in more expensive high-resolution cameras rather than cheaper, lower-quality ones, as this reduces the opportunity for perpetrators to manipulate or avoid detection. Regardless of the type of camera or its resolution, it is essential to identify the suspect, who will always deny their identity. The most effective method of identification is to use the same camera, at the same angle, and under the same conditions to capture comparative images for comparison, as proposed by Simonović and Pena (2010). Practically, this is very challenging. Therefore, if possible, one should examine the angles of video footage that show open parts of the body, profile, ear shape, or other noticeable features. However, problems always arise with masked perpetrators, or those covering their faces with so-called balaclavas. In such cases, attention should be paid to other characteristics, such as distinctive clothing items that stand out in those situations. Simonović and Pena (2010) further note that one method of identification via video surveillance is the anthropometric method developed in the United States. This method, with origins attributed to Alphonso Bertillon, has evolved with modern science and technology to provide the best possible results. According to this method, a series of at least nine anthropometric proportions are measured in a unit of measure suitable for the area where the measurements are taken. For us, this would be in centimeters.

As previously mentioned, a major problem is masked perpetrators captured by video surveillance. This issue is addressed by identifying distinctive clothing and footwear, as well as items in the possession of the perpetrator in the footage. Comparison is possible regarding clothing items (folds, shirts, t-shirts, jackets, pants, glasses, helmets, specific marks on clothing and footwear). As highlighted, the quality and resolution of the footage determine identification capabilities. Higher resolution results in more reliable and better forensic results. In such cases, no expense should be spared on good high-resolution cameras. It is the responsibility of criminal prosecution authorities to obtain the suspect's clothing and footwear through searches and inspections of objects, vehicles, spaces, terrain, and waste, and to perform comparisons based on comparative footage.

One problem may arise if the video camera is not placed in the correct or adequate location. In some cases, perpetrators of traffic offenses prone to criminal behavior are aware of the cameras installed in certain locations and blind them with headlights, thus preventing vehicle identification. It is not uncommon for object security to be handled similarly, with strong reflective lamps directed at the camera by perpetrators. In this regard, video surveillance must be combined with other protection systems. It should be noted that in international judicial practice are not unusual cases where perpetrators of criminal acts were convicted based on video footage of clothing from surveillance systems, as confirmed by sources from foreign literature (Simonović and Pena, 2010).

For every object or space being secured, an elaborate or study must be done to plan and design a specific security system. During project development, the needs for the security of the protected object must be considered, as well as previous knowledge, experiences, standard security measures, market developments in technology and techniques, and measures taken by agencies with available personnel and technical means. For objects of strategic importance and high material value, security success is enhanced by combining multiple different systems. Technical means improve measures for protecting public, social, or private property from violent appropriation, seizure, or destruction. When designing a quality security system, it is necessary to combine physical and technical protection measures. A comprehensive theory of security that defines all criteria for the production of technical means and technology, and their applications guaranteeing absolute security, has not yet been developed. Security always starts from minimal to maximum measures, the importance of the object or person being protected, and this dictates the cost of the security system. The cost influences the level of security. If the client is willing to pay for the highest level of security, then the best quality protection system should be provided. It is also important to remember that no security system is perfect, whether for objects or people, and there is no magical protection that guarantees absolute security. A possible model with the highest level of physical and technical protection involves organizing both direct and indirect security in several levels and concentric circles. The choice of system and its placement in specific circles depends on the object itself and access to it, as well as the primary protection goals (e.g., against burglary, terrorist armed attacks, fire, sabotage, or diversion within the object itself). Thus, before creating any project, an assessment of vulnerability and different forms of threats is made, followed by the creation of a model based on requirements, and finally, the project.

What are the minimal security measures for an object? These measures involve controlling access and movement of unauthorized persons and their identification, as well

as operational procedures within the protected space to prevent entry and movement. An imperative requirement for fire protection is also a part of all security elements. As previously emphasized, the protection system for objects is based on external and internal protection systems. External and internal protection fundamentally includes a combination of very complex measures and actions, as well as numerous technical and automated systems that adequately secure the protected space and objects, or their parts, as determined by previous security assessments (Ostojić and Knežević, 2003). The properties of technical systems must be based on the requirement for maintaining necessary security levels.

What is achieved by combining different technical protection systems in the global security system of an object or space? A suitable combination reduces the number of technical devices and equipment in the technical protection system. Proper assessment and solutions for technical security of protected spaces and objects reduce the number of guards or security personnel, while improving the efficiency of the protection model. Additionally, the technical protection system must minimize false alarms to the greatest possible extent. Modern equipment and systems now allow for long-term automatic and autonomous operation.

Conclusion

Designing and implementing technical protection for facilities has become a demanding and complex task, involving a diverse application of technical means and equipment. When designing and applying technical protection systems, it is crucial to consider the protection of fundamental human rights and freedoms, as well as adherence to legal provisions concerning the security of individuals and objects, and the protection of personal data. To ensure this, measures must be taken to prevent unauthorized recording. However, depending on the type of facility being protected, the element of surprise must also be respected. It is necessary to indicate that the facility is under technical protection and video surveillance, and to prominently display this information at entry and access points. Additionally, within the facility, it is important to install invisible motion detectors and hidden cameras, which detect intruders at depth and provide time for the physical security team to react and intervene. The goal is to surprise and thwart attackers by making them believe they have disabled visible sensors or cameras, thus creating conditions for an attack. Overcoming one line of obstacles does not mean the path to further attacks and achieving the facility's objective is open and secure. Coordinated preventive security measures for physical protection, including security personnel and the functioning of technical protection systems, prevent unpleasant surprises.

Experience and practice in applying protection systems have configured models of technical security systems and evaluated the minimum number of technical devices required for the system to function efficiently while maintaining a high level of protection in cases of burglary, terrorism and fireprotection. Therefore, it should be noted that the tactic of applying physical protection or physical security is especially developed, significantly reducing the shortcomings and weaknesses of technical protection, where the synergy of human and technology, and the use of modern technical elements of protection, come to full expression.

Literature

- Abazović, M. (2002). Državna Bezbjednost. Uvod i temeljni pojmovi. Sarajevo. Fakultet kriminalističkih nauka.
- Born, H., Caparini, M., Cole, E. (2007). Regulating Private Security in Europe: Status and Prospects. Geneva Centre For The Democratic Control Of Armed Forces (DCAF)Policy Paper – №20.
- Čakija D. (2011). Numerička analiza ugroženosti štićenog objekta od napada. Zagreb.Fakultet elektrotehnike i računarstva. Magistarski rad.
- Duvnjak, N. (2004). Fizičko-tehnička zaštita organizacija u službi obezbeđenja. Banja Luka. Defendologija. Vol. VII. Broj: 15-16. s. 55 – 62.
- Jovašević, D. (1998). Leksikon krivičnog prava. Beograd, JP Službeni list SRJ.
- Kešetović, Ž. Davidovć, D. (2009). Uporedni prikaz zakonodavstva privatnog sektora bezbednosti u zemljama EU I. Beograd. Strani pravni život. Broj 2. s. 235. – 251.
- Korajlić, et al. (2012). Istraživanje krivičnih djela. Sarajevo. Pravni fakultet.
- Mršić, D., Radić, G. (2023). Menadžment privatne sigurnosti u savremenom dobu, Zagreb. Volume 24. No. 3. National Security and Future. p.132 – 141.
- Ostojić, N., Knežević, P. (2003). Bezbednosna oprema u službi života (sredstva za zaštitu ljudi i objekata). Beograd. Novinsko izdavački centar „Vojska".
- Sabljić, M. (2022). Uloga privante zaštite u sigurnosti kritičnih infrastruktura. Završni rad. Karlovac. Veleučilište u Karlovcu – odjel sigurnosti i zaštite.
- Savić, D. (2013). Mjesto i uloga policijskih snaga u međunarodnim intervenicjama. Zagreb. Policija i sigurnost. God 22. br. 4. s. 479 – 493.
- Storm, K. et Al. (2010). The Private Security Industry: A Review of The Definitions, Available Data Sources, and Paths Moving Forward. US Department of Justice, Washington DC.
- Simonović, B., Pena, U. (2010) Kriminalilistika, Istočo Sarajevo, Pravi fakultet.
- Krivični zakon BiH, Službeni glasnik BiH, br.3/03, 32/03, 37/03, 54/04, 61/04, 30/05, 53/06, 55/06, 32/77, 08/10, 47/14, 22/15, 40/15, 35/18, 46/21, 31/23, 47/23.
- Krivični zakon Federacije BiH, Službene novine Federacije BiH, br. 36/03, 37/03, 21/04, 69/04, 18/05, 42/10, 42/11, 59/14, 76/14, 46/16, 75/17, 31/23.
- Krivični zakon Republike Srpske, Službeni glasnik Republike Srpske br. 64/17, 15/21, 89/21, 73/23.
- Krivični zakon Brčko Distrikta BiH, Službeni glasnik BDBiH, br. 10/03, 45/04, 06/05, 21/10, 52/11, 26/16, 13/17, 50/18, 3/24.

- Zakoni o prekršajima protiv javnog reda i mira Kantona Sarajevo. Službene novine Kantona Sarajevo broj 18/2007, 7/ 2008., 34/2020.
- Zakon o prekršajima Federacije BiH, Službene novine Federacije BiH br. 63/2014, 41/2022, 68/2022.
- IDEA (2016). Vodič kroz provjerena rješenja tehničke zaštite. Preuzeto 16. 11. 2016.
- sa: http://www.alarmautomatika.com/hr/download/31/
- A&S Adria. (2022). Security 50: Rast se vratio u industriju sigurnosti. https://www.asadria.com/security-50-rast-se-vratio-u-industriju-sigurnosti/#