Agata Tyburska
Mł. insp. dr hab.
Wyższa Szkoła Policji w Szczytnie,
Wydział Bezpieczeństwa
Wewnętrznegoa.tyburska@wspol.edu.pl

DOI: 10.35117/A_ENG_18_01_01

Assumptions of CPTED theory immunization in the critical infrastructure of the airport

Abstract: Terrorist acts are typical threats that provoke a crisis of considerable size not only in the country but also in the countries or regions. Terrorist interest will always be aroused by elements of state infrastructure, which are defined as essential for the daily functioning of people and public administration. Airports serving people and providing fast transport of goods are of particular interest to modern terrorists. Terrorist attacks targeting the airport infrastructure can cause both their destruction and damage, as well as initiate breakdowns that result in not only huge material losses, but significant deaths and damage to a substantial number of people. As a consequence, they may cause insecurity, panic and abandon the use of services guaranteed by carriers and airports. Developing real and effective protection plans, based on the results of research and analysis and good practice - allows for effective protection of a key airport area and, in a crisis situation, to minimize costs resulting from an attack. The Crime Prevention Trough Environmental Design (CPTED) concept of prevention of crime by shaping space focuses on physical space as an important factor influencing criminal behavior. This space is connected in various ways with the criminal act. The theory of shaping safe spaces assumes that criminals make a rational choice of purpose, and their decisions are supported by an analysis of the conditions existing in a given space (risk analysis). Their choice applies to both the places they prefer as the crime scene and the areas they avoid. The aim of the article is to present elements of the CPTED concept, which may be adopted in the protection of airport infrastructure

Keywords: Terrorism; Safe areas; Immunization; Critical infrastructure

Introduction

The nature of threats at the beginning of the 21st century made theoreticians and practitioners aware in the field of national security (state security), not only the need to verify knowledge regarding the identification and assessment of threats, but also the need to modify the existing concepts of protection of key state infrastructures. Terrorist activity focused mainly (in addition to systems operating in cyberspace), on the places where a significant number of people gather, as well as facilities, installations and devices that are important for the smooth functioning of the state, and as a consequence of its significant position on the international arena - it sets new directions for actions aimed at increasing the resilience of the targets of a potential attack. The elements of the state's transport infrastructure are becoming more and more frequent, and as a consequence people using this form of travel. Airports and seaports, air and sea vessels, railway stations, trains, metro stations - these are just examples of infrastructure elements in the interest of modern assassins. The special nature of threats affecting airports requires safety managers to intensify their protective activities, and thus use more and more new technologies and verify previously implemented solutions.

The concept of crime prevention through environmental design (CPTED) offers simple and effective solutions that increase the defensive nature of space, which is also reflected in solutions for the safety of persons and airport infrastructure.

Terrorist threats of critical infrastructure

Critical infrastructure is characterized by extremely complex, heterogeneous and independent assemblies (complexes) of objects, systems, and functions that are susceptible to various threats. The very number of critical elements, ubiquity and interconnectedness focus hackers or terrorists as a potential attack target, the effects of which will be so effective that they can force the government administration to change in internal or foreign policy. The effects of the terrorist attacks carried out at the beginning of the 21st century drew the attention of both theoreticians and practitioners associated with the area of security, the need to increase the resilience of infrastructure, which is crucial for the functioning of the state and its citizens. Researchers at the same time pay attention to the difficulties associated with the proper determination of this type of infrastructure and the extremely complex and dynamic nature of modern infrastructure.

Currently, most problem researchers see critical infrastructure as assets, services, and systems that support the economic, political and social life of the country, and whose importance is so significant that their total or partial destruction or damage could cause mass deaths; have a serious impact on the country's economy; cause other serious social consequences for the life and health of citizens or cause a serious problem for public administration [1].

In most countries, a systematic approach to the separation of the critical infrastructure of the state is used. Among the systems defined as critical, the transport system (air, water, road, rail) plays a significant role (from the point of view of the efficient functioning of the state and human safety), which is directly related to critical systems such as energy supply, energy raw materials and fuels, water supply, with a rescue or ICT system. Links and dependencies existing between elements of critical infrastructure and elements of other key infrastructures are sometimes so complex and complicated, that often make it difficult for them to properly diagnose and determine the level of criticality of the resulting nodes and key points. These complicated paths of connections and dependencies often go beyond the borders of the country, connecting with elements of the infrastructure of other countries - thus encumbering key elements with additional sensitivity. An important point is also the theorem derived by Alvin and Heidi Toffler that "*all parts of the system are (...) in a state of constant fluctuation. And they are extremely susceptible to external influences (...). The positive feedback loops multiply, which means that certain processes, once introduced into motion, begin to live their lives and, far from stabilization, introduce even more instability within the system (...). The convergence of internal and external fluctuations may lead to a complete collapse of the system or to its reorganization at a higher level* "[13]. Modern researchers emphasize that due to the size and scope of a potential goal, one cannot assume the possibility of 100% protection of all elements of critical infrastructure against possible threats [11].

After the coup of September 11, 2001, the governmental administrations of highly developed countries recognized terrorist attacks as a special type of security threats to the state. Currently, terrorism has an extremely strong impact not only on the sense and actual security of individuals but also affects the policy of governments, entrepreneurs and (indirectly) industry. Terrorist attacks recorded at the turn of the 20th and 21st centuries resulted in destruction or damage to public administration buildings, commercial facilities, metro or airport infrastructure, destruction of aircraft, and consequently the loss of life and health of many people. They also caused serious disturbances in the functioning of administration, pipelines and oil pipelines or airports in the air. According to analyzes - the most dangerous threats to national security are dangerous situations caused by cyber-terrorism. This results, for example from universal access to the Internet and the possibility of carrying out an attack without incurring any losses. As Krzysztof Liedel emphasizes, making

an attack on the Web does not require from the perpetrator special sophisticated skills with a significant percentage of anonymity [6]. This statement corresponds with the opinion formulated by Piotr Sienkiewicz, who, according to the opinion, cyber terrorism will become an increasingly common phenomenon due to low costs incurred by terrorists to prepare and carrying out the attack on the Web, the progressive globalization process, the use of the surprise effect, total anonymity associated with a low risk of detection [10]. The development of new information technologies and related cyber threats - due to the specificity and manner of functioning of sensitive elements - have a particularly strong impact on critical infrastructure. The likelihood of an attack in cyberspace, the size, and consequences of such attacks, are the result of connections (network connections) between key elements and the emergence of the information society. Threats in cyberspace are most often associated with the use of computer networks as a tool to paralyze or significantly limit the possibility of using national structures (e.g. transport, energy, government institutions) or to intimidate or enforce specific actions (or their abandonment) on the government or society) [3]. They are often the result of an unauthorized operation in computer systems and ICT networks both on the part of unauthorized persons and their users. The IT networks are currently used by most of the entities classified as critical infrastructure, including air traffic control systems, or customer service using this type of transport. According to Halina Świebek, cyber attacks on key infrastructure elements may "contribute to strengthening the classical attack effect by causing additional confusion and panic of the population (...), which as a result of the cascade spread of damages in electronic systems may pose a threat to the economy and public safety" [12]. Hence, among the situations most often mentioned as threatening the security of systems operating in cyberspace are activities that are of a computer sabotage (dissemination of viruses and worms, blocking systems), or attacks on a critical infrastructure consisting in interfering in its functioning. Therefore, contemporary terrorists increasingly use non-military (civilian) means, more easily available, and at the same time allow for a spectacular achievement of the assumed objective. It is worth emphasizing that terrorists perfectly estimate the risk when typing the goals of a potential attack. It is not difficult to predict that they collect all information on the resilience of critical infrastructure elements of countries that are interested in them. After recognizing the applied security (protection system) of an object, installation or device - in case of finding a high level of its resistance - they undoubtedly change the object of interest to focus destructive power on targets that they consider to be less protected, which favors fast reaching of the intended effect. Experience to date suggests changes in tactics: terrorists are increasingly attacking several elements of the state's infrastructure at the same time (or attacks occurring in a short period of time - the so-called "snowball effect") to make it difficult to carry out rescue operations, complicate chasing (determination of perpetrators), and in consequence increase the number of victims and the social response of attacks. The number, purpose, and range of modern attacks are more and more often inclined to take action to increase the resilience of critical infrastructure.
The airport due to its nature, resulting from:

a) accessibility for both external and internal users;
b) complexity of infrastructures (devices, networks, installations);
c) international character;
d) dynamic expansion of size and structure;
e) the need to cooperate with many entities operating the airport;
f) numerous connections and dependencies with other key elements of critical infrastructure (state infrastructures);
g) growing competition;
h) a significant number of people staying (concentrated) in a relatively small space

is particularly susceptible to carrying out acts of sabotage or a terrorist attack.

The concept of CPTED in the immunization of the critical infrastructure of airports

The contemporary nature of threats has made theoreticians and practitioners dealing with national security (state security) aware of not only the need to verify infrastructure knowledge and risk assessment but - what is important - forced the need to modify the existing concepts of key infrastructure protection of the state. Today, the protection of critical infrastructure is variously defined and interpreted. In the literature on the subject, the term refers most often to activities aimed at protecting "sensitive" systems and the structures that create them and includes: people, fixed assets and those elements of systems that are necessary for state security, the key infrastructure of cities, economic stability and public safety [8]. Some authors perceive the protection of critical infrastructure as specific strategies, decisions and readiness needed to protect, prevent and, if necessary, respond to attacks (including terrorist attacks) targeted at critical sectors, systems, and key goods and values [5].

Methods, means, and procedures applied in the framework of protection are aimed at preventing or (and) mitigating the effects of attacks on critical infrastructure caused by people (terrorists, hackers), natural disasters or technical failures. The protection of critical infrastructure should therefore be treated as a part of protection and national defense covering all types of prevention, preparation and response projects aimed at increasing the critical infrastructure's resilience to any kind of disturbances limiting its correct operation, as well as aimed at quickly restoring the functions performed in case of destruction, damage or failure. These projects include both legislative, educational and physical activities and technical, as well as all system solutions carried out at all levels of public administration, as well as implemented by the private sector, society and other entities acting for national security [14]. Critical infrastructure is embedded in a specific space. This space can be of a physical or symbolic nature. Physical space is defined as "the area perceived as a whole together with the objects in it" [15]. In real physical space are located real areas, buildings, devices, installations or networks forming the infrastructure of the municipality, city, district, voivodships, which make up the state's infrastructure. In turn, the symbolic space is referred to as the "whole phenomena of a specific kind" [15]. Therefore, the symbolic space can be associated, among others, with cyberspace, which consequently gives a wide range of possibilities to affect elements located in physical space. This impact may increase the resilience of a particular infrastructure element, or initiate situations resulting in its destruction, damage or failure. Wide access to the cyber world caused that this area was referred to as the new social space " [2].

The concept of Crime Prevention Through Environmental Design (CPTED) crime prevention by shaping space focuses on physical space as an important factor affecting the behavior of potential perpetrators of crime. This space may in various ways be related to the act of breaking the law. The theory of shaping safe spaces assumes that criminals rationally make a choice of the target and place of attack, and their decisions are supported by the analysis of the conditions existing in a given space, which are conducive (or not) to the decision to break the legal norm. The results of the conducted research indicate that anti-social behavior is concentrated in specific places, points or areas, which in turn - due to various factors - may hinder or facilitate the perpetrator's crime. These places can generate a subjective and at the same time a different level of sense of security as satisfactory or negligible for potential perpetrators/communities. Therefore, the choices made by the perpetrators of crimes concern both areas, facilities, devices or installations that they prefer as places "safe" for them to commit crimes, as well as places, which due to the high level of risk, usually avoid treating them as "endangered" places.

That is why the philosophy of Crime Prevention Through Environmental Design (CPTED) is based on the assumption of a logical and deliberate choice of goals by perpetrators of crimes

(assassinations), supported by meticulous risk analysis (profit estimation and start). One from the basic assumptions of the CPTED philosophy, it reflects the statement: "the greater the risk of being noticed, detected or caught, the lower the likelihood of committing a crime; the more effort is needed to commit a crime, the less likely it is to commit; the smaller the actual or probable profit from the crime, the less likely it is to commit it." [4].

The conducted research allowed to identify areas and specific places referred to as criminogenic. Researchers of the problem, using a specific methodology, are able to determine with great precision those elements of space that make it easier for a potential perpetrator to commit a prohibited act. Among the criminogenic elements relating to a specific space, the most frequently mentioned are: a large number of people simultaneously using the space; high degree of anonymity; lack of sufficient supervision, the difficult scope of observation, many possibilities (roads, exits, passages, etc.) for the escape of offenders. In addition, factors such as:

a) passages, tunnels, paths, designated routes - connecting two or more places, enabling anonymous movement of people (so-called traffic generators));
b) considerable size, dimensions of objects characteristic for places of residence of a significant number of persons (airports, commercial buildings, stadiums, places of manifestations and festivities) (so-called honeypots);
c) areas willingly chosen by the perpetrators for the places of attacks (so-called inflammatory points);
d) "forgotten" places as evidenced by their neglect and lack of any activity (so-called fear generators) [4]. The philosophy of activities known as Crime Prevention Trough Environmental Design (CPTED) dates back to the early 1960s. The protoplasts of the concept were E. Wood, J Jacobs. A significant contribution to its development was also made by such researchers as C. Jeffery; Oscar Newman or TimothyD. Crowe. The indicated researchers assumed that there are opportunities (tools) to transform the environment (space) in such a way that it would deter potential perpetrators, and thus limit the number of unlawful events. In the literature on the subject, CPTED is also referred to as a process consisting of several stages: design; creation; use and maintenance (management) of space. Hence, it includes "strategies, methods, techniques, and tools for shaping physical space and its effective use and management oriented on preventing and eliminating crime, anti-social behavior, as well as reducing the sense of threat" [7].

Among the constitutive features of CPTED, the following areas are indicated:

1. Access control;
2. Surveillance;
3. Technical security;
4. Maintenance status;
5. User support.

In the literature on the subject, you can also find the so-called 3D in shaping safe spaces, which relies mainly on "shaping physical space in the context of the normal and expected manner of its use by users. It takes into account the connection between functionality, use and management, and human behavior (...). is a simple way to assess space for useful users in determining if space is properly designed and used " [4].

The basic assumptions of the 3D concept of shaping safe spaces are based on three key premises:

1. prior determination of the purpose of a specific space (already at the stage of designing an architectural building, square, installation, etc.);
2. diagnose so-called social, formal, cultural and physical features of the space conditioning the occurrence of accepted behaviors;

3. design of a specific space and elements located there (objects, areas, devices, installations) gives the opportunity to control the behavior of people who are functioning (appearing) in a given space.

When preparing plans for the protection of key infrastructure, the following elements should be diagnosed: the initial purpose of the space (object, area, device); its current use and uses; forms of human activity occurring in a given area (object, device) and projected conflicts resulting from conducting various forms of activity in a given space. It is also necessary to examine to what extent human activity (requiring an increased scope of protection) reaches or focuses in the key places of the space (object, device, installation). Other interesting elements determining the security of objects and key devices is to examine the ways of delimiting areas with different levels of access, the range of visibility and the legibility of the signs and symbols used; conflicts that arise between the purpose of objects (areas and devices) and the way they are used.

From the point of view of design assumptions made for a specific space (object, device, network), it is necessary to determine to what extent the developed project allows preservation of originally planned functions, or allows or hampers users' activity resulting from the rights assigned to them and - what is important - in which scope allows you to control the behavior of people staying in a given space. Airports are a good example of the application of the elements of the Crime Prevention Through Environmental Design (CPTED) concept in increasing the resilience of the key element of the state. Modern airports are complex and complex infrastructures with a rich network of connections and dependencies with other elements of the state infrastructure. Efficient service of the airport is provided by many entities (institutions), which on the one hand ensures a high level of services provided, on the other hand, it brings additional challenges to those responsible for airport security.

According to Adrian K. Siadkowski, ensuring the safety of the airport will mainly concern "passenger service infrastructure and flight operations, i.e. objects, areas and devices important from the point of view of flight safety and civil aviation security against acts of unlawful interference" [9].In order to ensure passenger safety, service and prevent damage to or damage to airport infrastructure, a variety of solutions are used, in which the main principles characterizing the CPTED concept can be found, these are proposals for solutions in the field of:

a) determining, controlling access to specific places (zones) of the airport;
b) conducting airport infrastructure supervision (facilities, equipment, installations);
c) applying solutions referred to as technical security;
d) concern for a sufficiently high standard of infrastructure maintenance;
e) application of thoughtful solutions supporting users of various elements of airport infrastructure (passengers, service, technicians, etc.).

It is easy to see that access to various (designated) areas of the airport is limited according to the authorized authorizations and is subject to detailed control. Access control to specific places (zones) of the airport is aimed at preventing unauthorized persons from entering a specific area (object).

In the CPTED theory, access control is to "channel traffic and pedestrian traffic in order to limit access to particular parts of the terrain to people whose presence in these places is undesirable and unjustified by circumstances" [4]. Controlling access in this sense consists in separating specific zones and assigning rights to individual people to stay in specific places (areas, facilities, etc.). The solutions adopted in this area allow limiting the free movement of people around the entire facility (area), limit the number of people having access to critical elements of the facility, enable identification of people and, consequently, limit the possibility of committing a crime. For this purpose, various solutions are used, including physical and symbolic barriers as well as technical devices.

In the case of airports, the division into public zones, operational zones, restricted zones, and in them into specific parts (subzones) is used. Adrian K. Siadkowski, when analyzing the airport security plans, also points to the so-called separated zones and boundaries between these zones [9]. Public zones are separated in different ways from operational zones. For this purpose, both personal strength (physical protection), as well as technical means (in the form of barriers, fences) and electronic (video monitoring system), are used. In the author's opinion, the critical part is part of the restricted area of the airport, which includes: places available for departing passengers, as well as the place of transport, transfer, and storage of luggage. For the safety of this part of the airport and persons staying there, detailed checks of passengers and registration and inspection of baggage are carried out.

On the other hand, part of the airport designated for aircraft parking spaces when boarding passengers or placing loads and luggage in it is marked as a restricted zone. The limited system of assigning access to employees to particular zones at the airports resulting from the scope of duties prevents free movement of the entire infrastructure both to passengers and airport service. Conducting supervision over airport infrastructure is part of a comprehensive airport security system. The very concept of supervision is associated with careful observation and control. At airports, there is a rule of designating specific protection zones, referred to as internal protection, external protection, and peripheral protection. In order to ensure the security of the protected infrastructure, various methods, techniques, and tools are used, as well as procedures performed by security staff (performing patrols, physical inspections, etc.) as well as using new technologies.

To ensure the safety of passengers and airport infrastructure, different types of solutions are used as technical security measures. In the CPTED theory, technical security is defined as "securing a place or object that will prevent or impede the commission of a crime" [4]. As part of this type of measures are exchanged all kinds of physical security (fences, doors, locks) as well as electronic (alarms, watch, etc.). In the case of airport infrastructure, technical safeguards include not only various types of barriers and physical obstacles that prevent free, uncontrolled passage to individual zones, but also X-ray devices for scanned baggage and detection of dangerous objects (forbidden), X-ray devices and scanners used for screening liquids, explosive devices, magnetic gates or hand-held detectors for detecting metals.

Maintaining a high standard regarding the appearance (maintenance status) of the area is another concept of the CPTED concept, which also determines the safety of passengers and airport infrastructure. Care for the right look, maintenance of equipment and installations (fire-fighting, water-sewage, ventilation, etc.), fast and at the same time repairing damaged (unserviceable) elements of the port infrastructure, not only care for passenger comfort but also an important element of the security policy.

The direct connection with the maintenance of the appropriate standard (appearance) of the airport and its surroundings is noticeable with another element of the CPTED concept which is the use of well-thought-out solutions supporting users of airport infrastructure elements. Users of the airport are both passengers as well as technical service, employees and officers performing tasks for protection, administrative employees and representatives of external entities). In the theory of shaping safe spaces, user's support "consists in designing a space that prevents or hinders the use of this space in a manner inconsistent with the intended use and clearly indicates which behaviors are incorrect. It is a clear and unambiguous indication of how space should be used "[4]. The specific nature of airports requires, among other things, to thoroughly instruct passengers about what behavior is unacceptable, what kind of objects are subject to a strict carriage ban, how to behave in the event of a fire or other dangerous incident (eg a terrorist attack). A lot of information is passed on to passengers in the form of posters, information boards or simply diagrams, drawings and symbols due to the international character of airports and the resulting language barrier.

Conclusions

Terrorist acts are typical threats that provoke crisis situations of considerable size not only on the national scale but also countries or regions. A special interest of terrorists will always be aroused by elements of the state's infrastructure, which are identified as crucial for the everyday functioning of people and public administration. Terrorist attacks aimed at elements of critical infrastructure may cause damage, destruction, and failure resulting in not only enormous material losses but also death, bodily harm to a large number of people or environmental devastation.

Terrorist acts determined the approach to safety in air transport and contributed to the improvement of protective solutions, which certainly affects the resistance of airport infrastructure and passenger safety. Despite the passage of years, the concept of crime prevention through environmental design (CPTED) continues to play a key role in planning the protection of state infrastructure elements. It is also successfully used in the case of critical infrastructure elements of the state. Proponents of the theory of shaping safe spaces point to the huge potential and previously undiscovered possibilities of using the CPTED concept, as evidenced by the innovative solutions used in immunizing airports.

Source materials

[1] Atlas I .R, *21st Century Security and CPTED. Designing for Critical Infrastructure Protection and Crime Prevention*, CRC Press, London-New York 2008, s. 11.

[2] Bendyk E., Melomolekuły" „Polityka" 2006, nr 2574, s. 78-79.

[3] Gizicki W., *Państwo wobec cyberterroryzmu* (w:) *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna,* red. A. Podraza, P. Potakowski, K. Wiak, Wyd. Difin, Warszawa 2013, s.46-47.

[4] Głowacki R., Łojek K., Ostrowska E., Tyburska A., Urban A., *CPTED jako strategia zapewnienia bezpieczeństwa społeczności lokalnej*, Wyd. WSPol., Szczytno 2010, s. 17; 25;33;35;36.

[5] Lewis T.G.,_*Critical Infrastructure Protection in Homeland Security. Defending a networked nation*, Wyd. Wiley-Interscience, New Jersey 2006, s. 4.

[6] Lidel K., Cyberbezpieczeństwo – wyzwanie przyszłości. Działania społeczności międzynarodowej (w:) Bezpieczeństwo w XXI wieku. Asymetryczny świat, red. K. Liedel, P. Piasecka, T.R. Aleksandrowicz, Wyd. Difin, Warszawa 2011, s. 446-447.

[7] Łojek K., *Metodyka rozwiazywania problemów kryminalnych*, WSPol., Szczytno 2008.

[8] Radvanowsky R.,. McDougall A, *Critical Infrastructutre. Homelad Security and Emergerncy Preparedness*, Wyd. CRC Press, London-New York 2010, s. 4).

[9] Siadkowski A. K., *Bezpieczeństwo i ochrona w cywilnej komunikacji lotniczej na przykładzie Polski, Stanów Zjednoczonych i Izraela*, Wyd. WSPol., Szczytno 2013, s. 201.

[10] Sienkiewicz P., *Bezpieczeństwo w globalnym społeczeństwie informacyjnym* (w:) *Współczesny wymiar terroryzmu. Przeciwdziałanie zjawisku*, red. J. Gryz, R. Kwećka, Wyd. AON, Warszawa 2007, s. 93-96.

[11] Sullivant J., *Strategies for Protecting National Critical Infrastructure Assets. A Focus on problem-Solving,* New Jersey *2007,* s. 111.

[12] Świeboda H., Prognozowanie zagrożeń dla bezpieczeństwa informacyjnego (w:) Współczesny wymiar terroryzmu. Przeciwdziałanie zjawisku, red. J. Gryz, R. Kwećka, Wyd. AON, Warszawa 2007, s. 127.

[13] Toffler A., Toffler H., *Wojna i antywojna. Jak przetrwać na progu XXI wieku*?,Wyd. Kurpisz, Poznań 2006, s. 239.

[14] Tyburska A., *Ochrona infrastruktury krytycznej w Polsce – wyzwania w tworzeniu bezpieczeństwa narodowego*, „Zeszyty Naukowe AON". Dodatek, Warszawa 2013, 98-99.
[15] *Wielki Słownik Języka Polskiego*, www.wsjp.pl, 10.10.2017r.