SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2025
ORGANIZATION AND MANAGEMENT SERIES NO. 216

PREVENTION OF TERRORIST ATTACKS ON CRITICAL INFRASTRUCTURE ON THE EXAMPLE OF AN AIRPORT

Maciej KAŹMIERCZAK

War Studies University, Warsaw; m.kazmierczak@akademia.mil.pl, ORCID: 0000-0001-6985-3157

Purpose: The purpose of this article is to evaluate the state's critical infrastructure protection system using an airport as an example. Identifying potential weaknesses and suggesting improvements is a key part of this assessment. Selected research is presented to highlight the need to protect airports from terrorist threats and to illustrate the importance of inter-agency cooperation, resource allocation and advanced security measures in enhancing national security.

Design/methodology/approach: The research combines theoretical analysis and empirical investigation. Theoretical methods include a review of the literature and legal frameworks concerning critical infrastructure protection. Empirical research involves a diagnostic survey conducted through structured interviews with experts in national security and airport operations and survey technique using survey questionnaire tool. The data collected were analyzed qualitatively to synthesize key findings and recommendations.

Findings: The study reveals that while significant efforts have been made in securing airports, vulnerabilities remain due to accessibility and operational complexity. The findings highlight critical issues such as insufficient inter-agency coordination, inadequate allocation of resources, and the need for better threat anticipation capabilities. Recommendations are provided to address these gaps and improve the overall resilience of airports against terrorist attacks.

Research limitations/implications: The primary limitation of the research is the focus on airports as a specific type of critical infrastructure, which may limit the applicability of findings to other sectors. Additionally, reliance on expert opinions may introduce subjective bias. Future research could expand the scope to include other critical infrastructure types and incorporate quantitative data for broader validation.

Practical implications: The research offers practical guidelines for policymakers and airport operators to enhance the security of critical infrastructure. By implementing the proposed measures, such as advanced surveillance technologies and improved inter-agency coordination, airports can reduce their vulnerability to terrorist attacks. The paper also has implications for the development of standardized protocols in critical infrastructure protection.

Social implications: The findings have significant social implications by contributing to public safety and national security. Improved airport security can increase public confidence in the safety of transportation infrastructure, reduce the societal impact of potential terrorist attacks, and foster trust in government measures aimed at protecting citizens.

Originality/value: The originality of the paper lies in its comprehensive approach to evaluating airport security as part of critical infrastructure protection. By combining theoretical insights with empirical data from expert interviews, the paper provides a valuable resource for

http://dx.doi.org/10.29119/1641-3466.2025.216.13

academics, policymakers, and security professionals interested in enhancing national security frameworks.

Keywords: state security, critical infrastructure, airports, threats, protection.
Category of the paper: Research paper.

1. Introduction

Civilization or technological progress, in addition to its positive aspects, also has a negative character. The increased standard of living due to the development of electricity or ICT is associated with the dependence of the functioning of societies on their abilities. The electricity subsystem, which is a key component of any economy, can be disrupted, for example, by a terrorist act. Any disruption of the electricity supply can disrupt all areas of socio-economic life and create a local, regional and national emergency. The facilities of this subsystem include nodal transformer stations or power substations, the supervisory system of main transmission lines, power plants and thousands of kilometres of transmission lines. Another example is the ICT network, which is also very important for the smooth functioning of the state, its administration and business entities. Unfortunately, it is very susceptible to paralysis through, among other things, cyber-terrorist attacks (for example, on air traffic control towers at airports). Unfortunately, it is highly susceptible to paralysis through, among other things, cyber-terrorist attacks.

The subject of research presented in the article are the processes taking place in the national security environment, determining the need to strengthen defense capabilities in terms of protecting critical infrastructure facilities of the state. The cognitive purpose of the study is to check, verify and evaluate the functioning of the critical infrastructure protection system of the state and to demonstrate the need to protect facilities in the light of possible threats. The utilitarian goal was to specify conclusions and indicate recommendations aimed at improving the functioning of the critical infrastructure protection system for state security.

From the opinions of experts in the field of national security, a research hypothesis emerges, which shows that despite taking multi-directional actions in the field of crisis management, public administration operating at many organizational levels is not able to foresee all the threats that threaten the facilities and critical infrastructure.

The general research problem of the article boils down to an attempt to find an answers to the questions: What is the impact of threats to critical infrastructure facilities on the forms of their protection (on the example of an airport), and thus on the security of the state and its citizens? and how to prevent terrorist attacks on critical infrastructure?

The conducted research (Jakubczak, 2006) shows that the problem in providing adequate protection to critical infrastructure facilities and equipment whether point (such as airports) or linear may be the fact that they are relatively accessible and easy targets for attacks by terrorists, diversionary and special groups, as well as madmen or hackers.

In order to ensure the effective protection of critical infrastructure facilities and systems, steps must be taken to identify, that is, to determine on the basis of clear criteria, which facilities and systems constitute critical infrastructure of national, regional and local importance. The protection of critical infrastructure facilities and systems is a major challenge for governing entities in view of ensuring the security of the state as well as society as a whole. Therefore, the need to analyse this problem with detailed consideration of threats to critical infrastructure to organise means and ways that will be used to protect critical infrastructure systems and facilities using the airport as an example.

2. Critical infrastructure - literature review

Prior to the introduction of the term critical infrastructure into the national terminology related to crisis management (Lidwa, Krzeszowski, Więcek, Kamiński, 2012), there were such formulations as: facilities of particular importance for the security and defense of the state, areas, facilities, equipment, and transports subject to mandatory protection (Presch-Cronin, Marion, 2016).

However, regardless of the terminology, the protection of the state's critical infrastructure systems is increasingly based not only on the solutions operating in a given country, but primarily on international security standards, designed to ensure the continuity of their operation in the conditions of interconnected global undertakings, minimizing threats to these systems, and above all through mutual information and warning (Moteff, 2012).

In the area of critical infrastructure threats, terminological ambiguity does not prevail, so the consequence is that there is a situation in which a specific object belongs simultaneously to critical infrastructure and is particularly important for the security and defence of the state and is therefore subject to mandatory protection. Thus, there are suggestions that the concept of critical infrastructure should distinguish defence infrastructure (Lidwa et al., 2012), which would define facilities that are particularly important for state security and defence.

Defining facilities and installations critical for the functioning of the state is of fundamental importance in shaping the appropriate level of security for citizens. The rules for determining the systems and objects belonging to the critical infrastructure, which are real and cybernetic systems necessary for the minimum functioning of the economy and the state, are contained in a classified annex to the National Program for Critical Infrastructure Protection and only selected persons have the opportunity to check which of the objects belongs to critical infrastructure (NPFCIP, 2013). The emergency response system, based on the practical aspect that allows systems to be classified into groups to facilitate identification, is divided into system infrastructure elements, which include (Lidwa et al., 2012):

- normative-legal infrastructure,
- social infrastructure,
- IT infrastructure (infosphere),
- technical infrastructure (technosphere).

The above elements of the system infrastructure also include critical infrastructure systems defined by law. When talking about critical infrastructure systems, it should be remembered that these are objects, devices and installations constituting a given system, which are interrelated and dependent (Tyburska, 2010). Critical infrastructure systems are undoubtedly key facilities and systems from the point of view of the functioning of the state, on the efficiency of which the continuity of operation of specific public utility institutions depends), including power structures. These facilities and systems can be classified into 4 areas (Lidwa et al., 2012):

1. State defence.
2. Protection of the state's economic interest - such as airports.
3. Public.
4. Protection of other important interests of the state.

Pursuant to the Crisis Management Act (Act of 26 April, 2007), critical infrastructure includes systems and their functionally related facilities, including buildings, devices, installations, services crucial for the security of the state and its citizens and serving to ensure the efficient functioning of public administration bodies, as well as institutions and entrepreneurs.

The fundamental problem highlighted by the Crisis Management Law is ensuring that critical infrastructure is adequately protected from potential attacks, failures or other events such as assaults, unpredictable acts of nature or disasters that may disrupt the proper functioning of that infrastructure.

An important aspect, which is related to the protection of the most useful infrastructure, is also the minimization and neutralization of the potential consequences of the destruction and failure of the elements that make up a specific critical system, as well as its prompt restoration so that the situation does not adversely affect the state of security of citizens (Tyburska, 2010). Critical infrastructure protection is a significant problem due to its complexity, which results from multivariate threats, i.e.: failures, terrorist attacks, disasters, acts of nature or other unforeseen events.

Based on the provisions of the National Critical Infrastructure Protection Program, critical infrastructure protection is the process of ensuring its security including the pursuit of the expected outcome and continuous improvement. This process encompasses a significant number of task areas and competencies, involves multiple parties, and includes many activities aimed at ensuring functionality, following up on actions taken, and ensuring the integrity of critical infrastructure (NPFCIP, 2013). However, according to the Law on Crisis Management (Act of 26 April, 2007), critical infrastructure protection includes all activities aimed at ensuring the functionality, continuity of operations and integrity of critical infrastructure in order to prevent threats, risks or vulnerabilities, and to reduce and neutralize their effects, as well as to quickly restore this infrastructure in the event of failures, attacks and other events that disrupt its proper functioning. By critical infrastructure protection (Piątek, Truchan, 2013) they mean the part of protection and national defence that includes all kinds of projects of a preventive, preparedness and response nature, aimed at increasing the resilience of critical infrastructure to all kinds of disruptions limiting its proper functioning, as well as directed at the rapid restoration of the functions carried out in the event of destruction, damage or failure.

Critical infrastructure protection tasks include (Tyburska, 2010): issues of collecting and processing information that relates to critical infrastructure threats; aspects of developing and implementing procedures in the event of critical infrastructure threats; restoration of critical infrastructure; and the possibility of cooperation between the public administration and owners and owners and owners-in-ownership or subsidiaries of critical infrastructure facilities, installations or equipment in the area of critical infrastructure protection.

Preparing effective protection of critical infrastructure requires a comprehensive approach that takes into account the following areas in the organization of protection (Tyburska, 2010): physical protection; technical protection; personal protection; information and communication technology protection; legal protection; and assistance from the government party in the reconstruction of the damaged or destroyed element. Each of the aforementioned areas constitutes a complex system of activities requiring general and specialized knowledge, a wealth of experience including the use of so-called "good practices", the ability to analyze, as well as forecast threats.

The methods and measures used in critical infrastructure protection (Tyburska, 2010) are aimed at preventing or mitigating the effects of attacks carried out against a specific piece of critical infrastructure. These attacks can be caused by people (terrorists, criminals, hackers) or can be the result of natural disasters and technical failures (accidents involving hazardous materials like nuclear, radioactive, biological or chemical substances). According to the Critical Infrastructure Protection Program (NPFCIP, 2013), the protection system should be applied to all types of identified threats, whether natural, technical or intentional. The protection system should also be prepared to restore all functions performed by a particular piece of critical infrastructure in the shortest possible time.

In summary, critical infrastructure protection aims to safeguard those resources and assets of a key state that are indispensable to society and contribute to social well-being. Therefore, it focuses on protecting the key nodes and systems of any infrastructure that provides services to its communities - such as airports.

3. Terrorism vs. aviation terrorism

The phenomenon of terrorism still figures among the many problems that the international community has to solve today. For terrorists, it is a type of conducting asymmetric warfare, in which groups that are small in number, using sometimes unsophisticated means and simple methods, are able to shake the authorities and societies that have the most powerful armed forces and the highest level of civilizational development. It should be clearly emphasized here that all actions carried out by terrorists are criminal activities in the eyes of the law, as well as by socio-moral norms. By definition, terrorists take as victims innocent people, often of the same nationality as the terrorists, and the greater the enormity of the crime, the greater the social, political, sometimes economic, and certainly psychological and media effect of the terrorists' actions.

Definitions of terrorism, including terrorism in civil aviation, are nowadays presented in large numbers by various authors or state institutions around the world. Therefore, for the purposes of this work, a few of their examples have been selected, which, in the author's opinion, most closely reflect the essence of terrorism, including terrorism in aviation.

It is worth starting by presenting E. Zablocki's definition. According to his views, modern international terrorism, along with military and non-military (economic, social, environmental) threats, causes the greatest security threat in the world. He proposes to depict terrorism as a method of action involving the use of violence to obtain certain political, social or material benefits (Zabłocki, 2009).

The approach to the terminology of terrorism according to American views is presented, among others, by B. Hoffman in the publication Faces of Terrorism. According to this author, the essence of terrorism boils down to terrorists creating fear among societies in a conscious manner, maintaining the constant threat of a bloody attack in order to achieve the goals set by the terrorists. Hoffman also emphasizes the far-reaching psychological impact not only on the direct victims of attacks and their loved ones, but on the people and societies that learn about and experience it through the media, sometimes tens of thousands of kilometers away from the scene of the attack. It is in the sowing of fear, in the constant intimidation and creation of an atmosphere of psychosis among people attacked at random, completely unrelated to the cause for which the terrorists are fighting, innocent of the fact that they happened to be in that place, that Hoffman sees the essence of terrorism. On top of all this, he emphasizes the extremely important issue of media publicity, which is supposed to lead to terrorists achieving (Hoffman, 2001). It should be noted that similar interpretations of terrorism are presented by two important US state institutions: the State Department and the Department of Defense.

Nowadays in the literature one can find various types of terrorism, the classification of which is based on criteria including: ideological motivation, the acting entity, the tactics and purpose of the attack or the operating environment (Zabłocki, 2009).

Acts of air terrorism involve both attacks on aircraft and on aviation infrastructure (Liedel, 2013). It should be noted that in the available literature, aviation terrorism is often equated with air terrorism. It is therefore worth clarifying this issue as well. For example, according to P. Krawczyk, air terrorism is a narrower concept, as it indicates the airspace as the area where terrorist acts take place. Accordingly, air terrorism is a broader concept because it includes both airspace and the activities that secure it (Zabłocki, 2009).

The detailed classification of aviation terrorism threats includes attacks on air aviation (so-called air terrorism) and ground aviation (so-called air ground terrorism). In addition, it indicates how these attacks are carried out. For example, there are attacks aboard an aircraft, an attack by an aircraft on a ground (surface) object, an attack on an aircraft carried out from the air (occurs less frequently), an attack on an aircraft from the ground, and an attack on aviation infrastructure, usually at an airport, but also outside it.

Definitions of aviation terrorism presented by various authors or state institutions around the world are now numerous, and most often they differ only in minor details. However, the lack of an official definition in this area makes it difficult for individual states, as well as organizations, to prosecute and punish the perpetrators of terrorist attacks or aviation incidents. A way out of this situation is the recognition of the term “act of unlawful interference” in civil aviation.

Today, thanks to its qualities and structure, civil aviation is and will continue to be one of the most attractive targets for terrorists. Attacks targeting aircraft and the entire aviation infrastructure and the effects they have on society cause terrorists to achieve their goals while gaining worldwide publicity.

4. Legal conditions for civil aviation security (including airports)

The most important pieces of legislation in the area of countering terrorist attacks targeting civil aviation (including airports) are:

- Aviation Law of July 3, 2002 (Journal of Laws of 2002, No. 130 item 1112, as amended).
- Regulation of the Minister of Infrastructure on the National Civil Aviation Security Program of December 2, 2020 (Journal of Laws of 2021 item 17, as amended).
- Law on anti-terrorist activities dated June 10, 2016 (Journal of Laws of 2016 item 904, as amended).
- Law on the National Cyber Security System of July 5, 2018 (Journal of Laws of 2018 item 1560, as amended).
- Law on State Border Protection of October 12, 1990 (Journal of Laws of 2005, No. 226, item 1944, as amended).

- Decree of the Council of Ministers on the determination of the air defense command authority and the procedure for the application of air defense measures in relation to foreign aircraft disobeying the calls of the state air traffic management authority dated November 2, 2011 (Journal of Laws of 2011, No. 254 item 1522, as amended).

In the Aviation Law, the issue of terrorism and protection against it is contained primarily in Article 2, Section 20, and in Division IX "Civil Aviation Security" (Articles 186 to 189a), where requirements have been set out for, among other things, such important matters related to countering aviation terrorism as:

- operation of security guards and the Border Guard activities at airports,
- security control of passengers and freight,
- security requirements for agents and suppliers of supplies,
- the airport manager's security responsibilities, including considerations of the activities of the airport security service subordinate to him and the separation of protected areas at the airport,
- the drafting, implementation and control of the National Civil Aviation Security Program (NAPOLC).

The Border Guard activities carried out at airports include: the way security checkpoints operate, checking of airport security personnel (the way they act during inspections, their psychophysical state or possession of relevant certificates) and responding to incidents of public order disturbance at security checkpoints. In order to carry out its tasks, the Border Guard may use image recording systems located at the airport.

Tasks related to passenger and freight screening are performed under the supervision of the President of the Civil Aviation Authority in cooperation with the Border Guard, and carried out by: airport manager (this includes: passengers, cabin and checked baggage, non-passengers of the aircraft and their baggage, as well as mail, cargo and other materials transported by air); registered agent (for cargo and mail); and registered supplier of in-flight supplies (for in-flight supplies). The airport manager's tasks are carried out by the Airport Security Service (ASS).

The designation of a registered agent and a registered supplier of in-flight supplies is implemented by an administrative decision of the President of the Civil Aviation Authority after verification of civil aviation security requirements. In each case, the decision is supported by the opinion of the Commander of the relevant branch of the Border Guard. The prerequisites for obtaining the status of a security control operator are: positive completion of training, absence of negative prerequisites (positive opinion of the relevant Border Guard Commander) and obtaining a security control operator certificate.

The airport manager is responsible for designating operational and restricted areas and restricted areas of the airport and ensuring their proper security in order to prevent unauthorized access to them. Said zones should have designated passageways, which the airport manager agrees with, among others: Police, Border Guard, Customs and Fiscal Service and the President of the Civil Aviation Authority. Tasks in the area of airport security are carried out in cooperation with security services and concern, among others, the identification system (persons, vehicles) and security control related to access to restricted areas of the airport - concerns, among others, the detection of weapons, explosives and explosive (dangerous) devices. If there is a need to perform tasks that are beyond the competence of SOL, the airport manager is obliged to notify the Police and Border Guard. The list of zones and passages is specified in the airport security program.

An important piece of legislation describing general issues related to related to counterterrorism (including in civil aviation) is the Anti-Terrorist Activities Act, which has been in force in Poland since 2016. This law defines, among other things, what anti-terrorist and counter-terrorist activities are, as well as the manner of cooperation between the authorities responsible for carrying out these activities. These authorities are: Minister of the Coordinator of Special Services, Head of the Internal Security Agency, Commander-in-Chief of the Police, Commander-in-Chief of the Border Guard and Commander-in-Chief of the Military Police.

Another important document is the Law on the National Cyber Security System, which is a response to new terrorist threats. It identifies in Article 4 key service operators and the Polish Air Navigation Services Agency (PANSA) as participants in the system. Annex 1 of the law details which air transport entities are key service operators, which include an air carrier (an air transport company with a valid operating license), an airport operator (a management entity entered in the register of civil airports) and an entrepreneur who performs services for air carriers regarding, among other things, the handling of passengers, baggage, cargo, goods or mail, as well as the airport apron and aircraft, and security control tasks. Tasks for these entities to function in the national ceber-security system are specified in Chapter 3 (Articles 8 through 16). They concern, among other things, the need for key service operators to implement a security management system in the information system to ensure, among other things, the collection of information on cyber security threats (estimating the risk of an incident) and its impact on the provision of a key service. All these measures are aimed at avoiding terrorist attacks in cyberspace.

To sum up the consideration of Polish law in the field of civil aviation security, it should be emphasized that an important role is played here by the law regulating aviation activities Aviation Law (along with implementing acts), and the issues contained therein are in line with the with European Union legislation. On the other hand, detailed provisions on civil aviation security are contained in the National Civil Aviation Security Program, which is set forth in the appendix to the Decree of the Minister of Infrastructure dated December 2, 2020. Nevertheless, in the author's opinion, some provisions of the cited legal acts need to be amended and clarified (this applies especially to the discussed issues of actions against aviation terrorism). However, it should be borne in mind that the mere formulation of regulations is not enough and it is necessary to comply with them.

5. Organizational and technical methods of countering terrorist attacks at the airport

Counter-terrorism in civil aviation aims to ensure the safety of passengers, flight personnel and all other persons who are at risk. This is made possible by the introduction of effective security systems and the operation of relevant services at the airport and on board the aircraft.

5.1. Airport security services

One of the most important elements of the security system against terrorism are the relevant services at the airport and the aircraft crews, sometimes reinforced by security guards. Among the services that provide security against terrorist attacks terrorist attacks and leveling their potential effects at the airport include: Airport Security Service; Border Guard; Police; Airport Fire and Rescue Service and additional services from outside the airport (such as the Office of Anti-Terrorist Operations of the Police Headquarters or mine patrols).

The main service responsible for airport security is the Airport Security Service, which protects the area of the entire airport. It performs its tasks in the form of direct personal protection carried out by officers of this formation, as well as through other activities. These include the constant supervision of signals transmitted and collected in electronic devices and alarm systems located at the airport. The basic activities that are carried out by the Airport Security Service primarily include:

- security control of passengers, crews and baggage,
- protection of restricted areas of the airport,
- checking passes (authorizations) of persons at checkpoints between individual airport zones,
- inspection of the technical condition of the airport fence.

Currently, to detect airport security threats, the Airport Security Service uses specialized, state-of-the-art equipment including, among others: stationary and hand-held metal detectors, X-ray equipment for cargo and baggage screening, explosives identification equipment, and uses trained service dogs to detect weapons and ammunition. The principles of some of the equipment designed for airport security screening are described in the next section of the article.

The second important service performing airport security tasks is the Border Guard. In addition to its basic tasks related to the protection of the state border at an international airport, this formation carries out activities with regard to countering terrorist attacks in accordance with the provisions contained in the Act of July 3, 2002. Aviation Law (as amended) and the Border Guard Act of October 12, 1990 (as amended).

The Border Guards at the airport focus their activities on a number of important activities related to preventing terrorist attacks. One of them is to prevent the smuggling of explosives and hazardous substances across the border. This is carried out, among other things, through effective control of passengers, baggage, shipments and goods. Pyrotechnic reconnaissance is also of great importance in this regard and the proper securing of aircraft prior to takeoff, which is particularly important to ensure the safety of passengers during flight. Added to this is the prevention of illegal border crossings. No less important is also ensuring public order at the airport and recognizing and, if necessary, neutralizing terrorist threats. In order to be able to effectively carry out the above tasks at the airport, Border Guard officers have appropriate powers over passengers and freight control. These boil down to, among other things, the ability to conduct personal inspections, inspect luggage and check cargo at airports. Also important is the observation of arriving and departing passengers who may pose a terrorist threat to the airport. Border guards at the airport work closely with other services to counter terrorist threats.

Another service responsible for security at airports is the Police Department. The police station at the airport mainly carries out tasks related to common crimes, but in a crisis situation, officers of this station can be engaged to counter terrorist activities, among others. However, the Police as a whole formation is extremely important in the fight against terrorism due to the availability of specialized anti-terrorist and counter-terrorist services (https;//www.ulc.gov.pl). A very important role is played by the Police during the occurrence of the aforementioned crisis situation that a terrorist attack at the airport can be. Then, thanks to police negotiators, negotiations are conducted with the terrorists, and when they do not bring the expected results, police counter-terrorists come into action. The main anti-terrorist unit is the Central Counter-Terrorist Subdivision of the Police Anti-Terrorist Operations Bureau and the Independent Counter-Terrorist Subdivisions of the Police operating in all provinces. These sub-divisions are responsible for conducting counter-terrorist operations under conditions of special threat, when there is a need to use specially trained officers and specialized weapons and equipment, as well as appropriate tactics adapted to the object where the terrorist attack takes place (including at airports). One of the police's most important partners in these operations is the Border Guard, as it has sizable forces and resources and is familiar with the vital infrastructure elements that serve port security.

The last of the services discussed, but very important from the point of view of the safety of airport operations, is the Airport Rescue and Firefighting Service. The scope of this service is regulated by a decree of the minister responsible for transport. This is an important airport security body is primarily tasked with securing all aircraft operations related to takeoffs and landings taking place at an airport. Thus, the Airport Rescue and Firefighting Service undertakes actions necessary to eliminate threats to human health and life and infrastructure at the airport. Specific tasks carried out by the Airport Rescue and Firefighting Service may include: securing fire-hazardous operations on the tarmac (e.g., refueling aircraft with passengers); or securing an emergency landing of a damaged aircraft. The task of conducting rescue and firefighting operations at the airport and the adjacent operational area is important.

The primary body responsible for planning and organizing airport security is the Airport Security Team. This team is appointed by the airport manager on the basis of the obligation under the Law of July 3, 2002. Aviation Law and the Decree of the Minister of Infrastructure of December 2, 2020 on the National Civil Aviation Security Program.

The main purpose of this team is the joint action of all entities operating at the airport to prevent the preparation of and occurrence of acts of unlawful interference, including terrorist attacks. The Airport Security Team meets periodically, at least once a quarter, and the content of its work during such meetings is mainly to agree on specific actions proposed by the entities responsible for security at the airport within the scope of their competence. On the other hand, in the event of a crisis situation at the airport, and such a situation may be a terrorist attack, a crisis staff prepared in advance (also by the airport manager) comes into action. This staff, once activated in an emergency mode, directs all entities involved in resolving the crisis situation. The chairman of the crisis staff is usually the airport manager, and sometimes the director of security. The operation of the crisis staff is based on the same legal basis as the operation of the Airport Security Team.

5.2. Technical anti-terrorism security systems at the airport

A very important element related to airport security is technical systems, whose task is primarily to support all activities carried out by airport services to counter terrorist attacks at airports. Among the security control systems we can include: systems for the control of personnel, crews, passengers and baggage; access to specific regions (areas) and facilities of the airport; courier shipments, cargo (goods) and mail, or people employed at the airport. At the same time, it should be borne in mind that the aforementioned systems should provide an effective, unified and integrated airport security management system while remaining immune to any attacks by terrorists (Dilling, 2005).

The technical means used to control people are usually stationary metal detectors, as well as trace analysis equipment. Nowadays, the use of gates with explosives trace analyzers is also a good option. They are usually located in front of the entrance to the operational area of the airport behind the security checkpoints. The most common devices of this type on the market are Sentinel II and Entry Scan.

An important element of security screening at airports is the metal detection gate, the principle of operation of which is related to the impact on the person located in the gate an alternating low-frequency electromagnetic field Detection of dangerous objects (metals) is the result of interference generated by the magnetic field coil. The quality and sensitivity of these devices makes it possible to precisely and accurately determine what type of metal is to be detected and what is to be ignored (e.g., allows detection of small blades that can be a danger to the crew and passengers of an aircraft).

Another important part of the security procedure is the screening of each passenger's carry-on baggage, which is done with a scanner that uses X-rays. This allows the operator of the machine to see exactly what has been packed in the hand luggage. Since each item has a different density, the operator can clearly distinguish between soft and hard items (e.g. glass bottles, metal or explosives). Nowadays, modern devices of this type can identify potentially dangerous items themselves.

Extremely important from the point of view of protection against terrorism is the ability of the services to detect non-metallic objects that can be a tool in the hands of terrorists. Most often, terrorists may place such items in carry-on luggage, and it cannot be ruled out that terrorists carry them in person by stealth Hence the great interest of the services in having devices for detecting such items. Manufacturers, meeting such demand, offer devices for sub-millimeter waves with an operating frequency of about 600 GHz. Another type of such devices are those operating on the principle of low-energy X-ray backscattering. All this makes the level of security even higher.

Security control systems related to airport security also consist of technical devices whose task is to detect intruders (dangerous situations) and immediately alert airport security services of the events. Among the most common we can include: motion detectors, buried sensor cable and overhead, radars and microwave barriers.

The operation of the buried sensor cable is based on the principle of interference with the detection field caused by an unwanted person. The interference depends on the mass and speed of movement of the individual in question. This eliminates false alarms caused, for example, by small animals.

Sensory cable infiltration is designed to prevent unwanted people from trying to get over the top of the fence. At the same time, interference caused by, among other things, ground vibrations caused by passing cars or adverse weather conditions (precipitation, wind) is excluded (https://ale-wiedza.pl).

The radars used for protection allow precise determination of the direction, distance and size of the detected object. Radars can monitor a fairly large area, so their operating range can be from a few hundred meters to 10 km.

The principle of the microwave barrier is that an invisible beam of energy in the microwave frequency range travels between the transmitter and the receiver. Any change in signal amplitude between these devices is immediately read and analyzed for the physical characteristics of the object that caused the interference. As a result, the system can detect an individual running, walking or crawling, and objects that do not pose a threat are considered a false alarm (https://atline.pl/kategorie-oferta/bariery-mikrofalowe/).

The above systems largely minimize the risk of unwanted people entering the airport area. However, it should be remembered that they are not perfect and there is always a risk of unlawful intrusion into the protected area or the occurrence of a false alarm.

5.3. Innovative technology as part of counter-terrorism at the airport

Ensuring a high level of security is paramount for any aviation organization. At airports, in order to improve security levels, electronic systems are increasingly being used to support security and service operations. It should be borne in mind that innovative technical systems for airport security play a key role in the process of detecting manifestations of acts of unlawful interference and enable effective counteraction.

An innovative latest-generation access control system for use at airports is AC2000 Airport (Figure 1). It provides integration of other security systems from various manufacturers, including surveillance systems (including video), intrusion or assault signaling and fire alarms. These systems are managed centrally and function as a single multifunctional security system. The solution's capabilities, integration and multifunctionality make the AC2000 Airport system widely applicable in airport security.

This system makes it possible to direct the movement of passengers to the various check-in counters located in the airport, as well as to control the movement of luggage. This is possible with the use of special identification cards. In addition, the AC2000 Airport system makes it possible to control and track the work of airport security services, improve the service of airport service cells, and facilitate the enforcement of order regulations with respect to passengers. According to experts, the AC2000 Airport system is currently the best tool that enables safe and efficient management of the airport both operationally and economically, as it provides a high level of security for the entire facility thanks to innovative software applications.

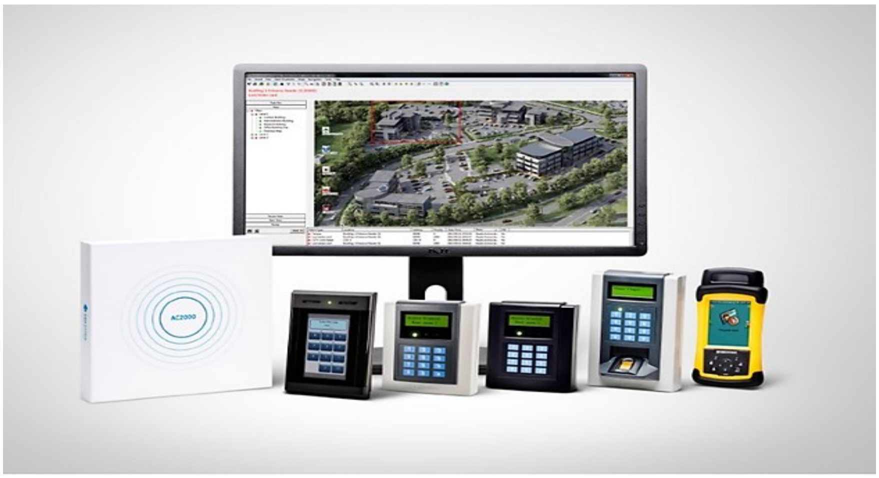

Figure 1. AC2000 Airport system components.

Source: https://lanster.com/systemy-zabezpieczajace-z-rozproszona-inteligencja-cem-systems/.

Next-generation CEM equipment is a smart and innovative technology, as its readers create the possibility of multi-level security management throughout the airport. This allows for efficient and effective control of, among other things, the boundaries between spaces (land and air), passageways (gates) for personnel, the operation of the air traffic control tower or other infrastructure functionally related to the airport. The possession of internal databases by the CEM readers makes it possible to continuously (24/7) verify the validity of ID cards off-line, and thus it is possible to control access to sensitive areas of the airport without any downtime. Equipped with touchscreens, CEM's emerald multifunction terminals enable the latest intelligent features of the AC2000 Airport system to be implemented at any point in the airport where they are deployed. This makes the emerald terminals both integrated readers, controllers and VoIP intercoms, which enable, using the appropriate applications (software), directly from the controlled passageways, the secure use of key AC2000 Airport system functions.

Access to protected areas of the airport using additional security such as a PIN code is enabled by modern and intelligent S610 readers, which, synchronized with an LCD display, inform security of the prohibition of access to certain areas of the airport, e.g. by the expiration of a card or the barrack of the appropriate authorization to a particular airport area. Another solution is the S610f biometric reader, which provides protection by verifying the validity of the identification card with confirmation of the PIN and the match of the fingerprint of the cardholder in question. Depending on the required level of security, one can choose the appropriate combination of these authorization criteria - from confirmation of the relevant PIN code alone, or additionally with simultaneous verification of the card bearers' fingerprint matches (https://lanster.com).

A new solution to improve airport security is an innovative magnetic sensor technology that aims to provide better and reliable ways to observe vehicle traffic. The use of this technology is expected to help airports eliminate runway incursion incidents. ISAMEL has developed a system to enhance protection and security in the harshest weather conditions and in places where traditional monitoring systems cannot truly assess the situation. ISAMEL's sensors are created to work as part of so-called advanced ground traffic management and control systems Advanced Surface Movement Guidance and Control Systems – ASMGCS (www.trimis.ec.europa.eu.)

6. Analysis of on research results – assessment of critical infrastructure systems and facilities

The conducted research shows that the economic and social role of critical infrastructure requires a systemic approach to its protection, while ensuring its normal functioning. This is related to organizing such solutions that are adequate to the needs posed by the population. Broad expectations of the reliability of critical infrastructure make it necessary to involve various entities in its protection, which should have sufficient competence, knowledge and tools to counter threats by reducing the possibility of their occurrence and to remove their consequences, including restoring the functionality of this infrastructure.

The extent of preparation of entities protecting critical infrastructure is extremely important. These activities must be subject to control, which can be implemented by preparing, conducting and analyzing Multimedia Decision Training. However, due to the declarative and unsanctioned nature of the participation of critical infrastructure protection entities in the infrastructure protection program, its organization may be the subject of exercises, such as in the form of decision-making games, recommended by the Government Security Center (GSC).

In order to be able to assess the security and security methods of critical infrastructure systems and facilities (such as the airport), 60 respondents were asked to express their opinion on this aspect. The metric shows the characteristics of the survey group in terms of gender, age, education, place of residence and affiliation with uniformed formations. The study included 18 women, accounting for 30% of the respondents, and 42 men, accounting for 70%. The respondents participating in the study formed a very diverse group in terms of age. There were no individuals under the age of 20. The largest group, nearly half of all respondents, were middle-aged 31-40 year olds – 49%. Slightly smaller was the percentage of those aged 21-30 – 21% and 41-50 – 23%. The smallest group was made up of people over 50 years old – 7%.

Taking into account the education of the respondents, the largest group, 65%, were those with higher education. One in five respondents – 20% have so far obtained a secondary education, and only 4% a vocational education. The largest group of those taking part in the survey were those living in the countryside – 30%, 32% live in a city of up to 20,000 residents. One in five respondents lives in a city with a population of 20,000 to 50,000. The remaining 18% of respondents live in a city with a population of 50,000 to 100,000. Most of the survey participants serve in the Polish Army – 54%, 25% in the Police, 14% in the Border Guard, and only 7% in Airport Security Service.

The results of the respondents' opinions on the protection of critical infrastructure presents figure 2.

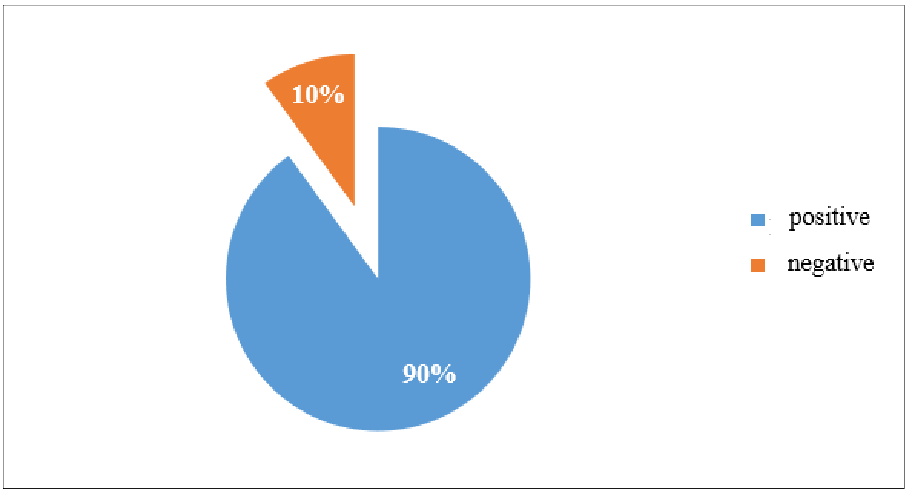

Figure 2. Survey group opinion on the protection of critical infrastructure in Poland.

Source: own study.

Substance-related questions focused on survey participants' opinions on: critical infrastructure protection (including facilities and systems), potential threats to Poland's critical infrastructure, and the hierarchy on the issue of threats related to the protection of critical infrastructure facilities and systems. As many as 90% of respondents believe that the protection of critical infrastructure in Poland is adequate, only 10% believe that it is inadequate, and in justifying their choice, this group recognizes that some elements of this infrastructure are not protected at all, or that protection is reduced to technical or mechanical security only. One person indicates that there are too few IT specialists – programmers who can design security systems, and that it is too expensive to operate security and protection systems. Figure 3 presents the results of respondents' opinions on the protection of critical infrastructure facilities and systems.

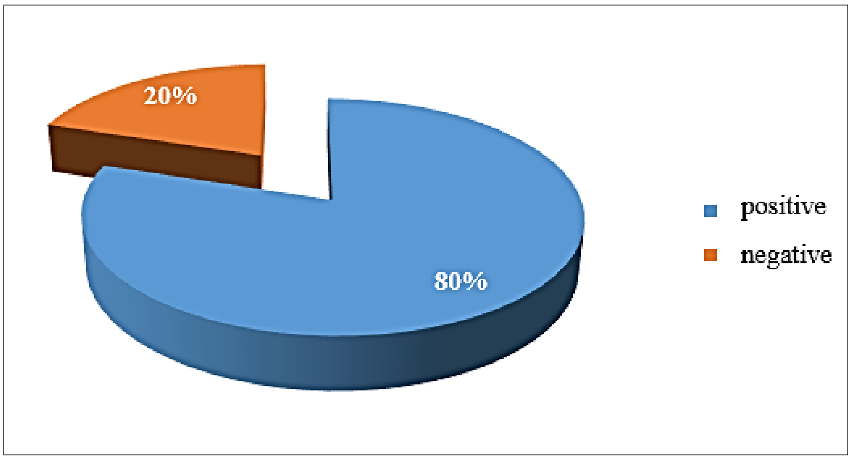

Figure 3. The opinion of the survey group on the protection of objects and systems of critical infrastructure in Poland.

Source: own study.

In the case of protection of objects and systems of critical infrastructure in Poland, as many as 80% of respondents said that it is sufficient. Unfortunately, one in five respondents felt that this protection was not adequate. Among the reasons cited here was the weakness of safeguards regarding infrastructure related to the provision of water to residents, including insufficient protection of deep wells, transportation systems. Respondents also made comments as to poor security regarding internet access. Table 1 shows potential threats to Poland's critical infrastructure as perceived by respondents.

Table 1.
Potential threats to Polish critical infrastructure in the opinion of respondents

Type of threat	n	%
Natural hazards	42	70
Accidental threats	8	17
Informed threats	10	13
Total	60	100

Source: own study.

The largest group of people said that Poland's critical infrastructure is most threatened by disasters and natural hazards. This is the opinion of 70% of respondents. 17% of respondents indicated accidental threats, and 13% indicated deliberate (intentional) threats.

The next question asked which system respondents believe is most at risk? Among the most threatened systems, respondents cited the energy, energy resources and fuel supply system at 42%, the financial system at 26%, the water supply system at 12%, the transportation system at 9% and the food supply system. 3% of respondents each cited the communications system, the health care system, the emergency system, the system that ensures the operation of public administration, and the system for the production, storage, storage and use of chemical and radioactive substances as the most endangered system.

Another question asked about the most important issues in critical infrastructure protection. The most important issues in critical infrastructure protection were considered by respondents to be cooperation between the public administration and owners and owners and owners-in-ownership or subsidiaries of critical infrastructure facilities, installations or equipment in terms of their protection – 33%, restoration of critical infrastructure – 25%. A slightly smaller percentage considers the collection and processing of information on threats to critical infrastructure to be the most important aspect – 22%, and the development and implementation of procedures in case of threats to this infrastructure – 20%. Analyzing the degree of importance of forms of protection in the event of an emergency, the largest number of people considered technical protection – 32%, physical protection – 24%, ICT protection – 22% and personal protection – 12%. The least important, in the opinion of respondents, is legal protection – 2% of respondents believe so, as well as assistance from the government side in the reconstruction of the damaged or destroyed element - as indicated by 6% of respondents.

Considering 10 aspects, such as analyzing the degree of threat to the facility, assessing the current state of security, ensuring the safety of the occupants, controlling the movement of people, controlling the movement of materials, controlling the technical security of the facility, complying with regulations and procedures, ensuring the reliable operation of the facility or system, protecting against theft, damage, vandalism and maintaining official secrecy, respondents were asked to prioritize them. Table 2 shows this hierarchy for facilities, and Table 3 for critical infrastructure protection systems.

Table 2.
Importance of each aspect in protecting facilities

Aspect	Importance of aspect				
	1	2	3	4	5
Analysis of the degree of threat to the facility	74%	18%	5%	3%	0%
Assessment of the current state of protection	64%	14%	15%	4%	3%
Ensuring the safety of the occupants of the facility	0%	0%	0%	18%	82%
Control of personnel movement	24%	19%	40%	10%	7%
Control of material movement	6%	14%	62%	10%	8%
Control of technical security of the facility	41%	31%	13%	8%	7%
Compliance with regulations and procedures	66%	19%	15%	0%	0%
Ensuring reliable operation of the facility	11%	16%	51%	20%	2%
Protection against theft, destruction, vandalism	8%	20%	39%	19%	14%
Maintaining service secrets	2%	3%	14%	21%	60%

Source: own study.

Table 3.
Importance of individual aspects in system protection

Aspect	Importance of aspect				
	1	2	3	4	5
Analysis of the degree of threat to the system	18%	66%	6%	3%	7%
Assessment of the current state of protection	8%	10%	74%	5%	3%
Ensuring the security of the system	2%	18%	58%	19%	3%
Systematic control of the system	2%	3%	19%	10%	66%
Control of system repairs	18%	20%	42%	16%	4%
Control of authorizations of people working in the system	0%	29%	44%	24%	3%
Control of technical security of the system	1%	0%	0%	26%	73%
Compliance with regulations and procedures	5%	20%	52%	20%	3%
Ensuring reliable operation of the system	0%	21%	27%	39%	13%
Protection against theft, destruction, vandalism	0%	3%	17%	26%	54%
Maintaining service secrets	8%	11%	21%	39%	21%

Source: own study.

The most important in the protection of the system according to the opinion of the respondents is the control of technical security of the system, its regularity and protection against theft, destruction, vandalism. A point less important is maintaining official secrecy and ensuring reliable operation of the system. Of medium importance to respondents is the evaluation of the current state of security, ensuring the security of the system, compliance with regulations and procedures, control of the authority of people working in the system, and control of system repairs. Respondents considered the analysis of the degree of threat to the system to be the least important aspect.

7. Conclusions

The growing importance of critical infrastructure facilities and systems to state security derives from their strategic importance in sustaining the uninterrupted functioning of the state under modern threats. The threat of a terrorist attack, regional instability near national borders, the use of weapons of mass destruction or the potential possibility of a crisis situation requires increased efforts to prevent, limit or minimize the loss and destruction they will bring with them. Critical infrastructure systems and facilities are particularly important for the proper functioning of state security. Their destruction can negatively affect the sense of security in citizens and contribute to the weakening of our country. Particularly dangerous are natural, civilization and terrorist threats hence the need to develop specific systems for the protection of critical infrastructure objects and systems. Their security is provided by physical, technical, ICT and legal protection. To make this protection as effective as possible, the constantly updated and responsive Act on crisis management obliged the Government Security Center to create a National Program for the Protection of Critical Infrastructure.

This article was an attempt to examine the need to protect critical infrastructure systems and facilities – such as airports resulting from their strategic importance and their security in light of possible threats.

The objective presented in the paper, the main research problem and the considerations undertaken in the article allowed the author to formulate the following general conclusions:

1. Threats to critical infrastructure systems and objects have a significant impact on the forms of their protection (depending on the projected threat to the object, appropriate measures are applied).
2. Of vital importance in ensuring security at airports and the entire aviation infrastructure are technical security systems. Airports use various types of X-ray equipment, stationary metal detectors, gates with explosives trace analyzers and, increasingly, biometric passport readers to screen passengers and luggage. However, it should be remembered that even 100 percent efficient systems and technical devices that use the latest technology cannot replace the operator, who makes the most important decisions.
3. A very important role in ensuring airport security, are the security services, which are responsible for specific tasks related to ensuring the safety of passengers. These include, among others, the Police, Border Guard, Airport Security Service.
4. Taking into account various factors and aspects and possibilities of terrorist activities, it can be assumed that the degree of terrorist threat in aviation will continue at least at the current level. However, it should be borne in mind that in the future the challenge for aviation will be not only legal-competitive disputes over the assessment of specific examples of air terrorism, but primarily security, i.e. security in airports, terminals, airports and their surroundings.
5. Security of critical infrastructure systems and facilities will be provided by physical, technical, personal, ICT and legal protection. At the same time, respondents considered the most important aspect in protecting facilities to be ensuring the safety of people on the premises and maintaining official secrecy. In turn, the most important aspect of system protection is the control of technical system security, its regularity and protection against theft, destruction, vandalism. Slightly less important is the maintenance of official secrecy and ensuring the reliable operation of the system.

In summary, the multifaceted nature and voluminousness of the presented content contributed to limiting the work to only the most relevant elements and narrowing the analysis by selected issues. In the author's opinion, the presented study can become an inspiration to explore the subject matter and serve for further scientific research.

References

1. Act of 12 October 1990 on the Border Guard (Journal of Laws of 2005, No. 226, item 1944, as amended).
2. Act of 26 April 2007 on crisis management (Journal of Laws of 2017, No. 91, item 209, as amended).
3. Act of 3 July 2002 on Aviation Law (Journal of Laws of 2002, No. 130, item 1112, as amended).
4. Dilling, M. (2005), Przeciwdziałanie atakom terrorystycznym w cywilnych portach lotniczych. In: S. Zajas, A. Glen, P. Krawczyk, T. Zieliński (eds.), *Przeciwdziałanie atakom terrorystycznym na lotniskach wojskowych i cywilnych* (p. 35), Warsaw: AON.
5. Hoffman, B. (2001). *Oblicza terroryzmu*. Warsaw: Grupa Wydawnicza Bertelsmann Media, pp. 32-34.
6. https://ale-wiedza.pl/kable-sensoryczne-systemach-ochrony-charakterystyka/, 23 October 2024.
7. https://atline.pl/kategorie-oferta/bariery-mikrofalowe/, 23 October 2024.
8. https://lanster.com/systemy-zabezpieczajace-z-rozproszona-inteligencja-cem-systems/, 23 October 2024.
9. https://trimis.ec.europa.eu/project/intelligent-surveillance-and-management-functions-airfield-aplications-based-low-cost#tab-contact, 23 October 2024.
10. Jakubczak, R. (2006). *Bezpieczeństwo narodowe Polski w XXI w.* R. Jakubczak (ed.). Warsaw: Bellona, p. 355.
11. Lidwa, W., Krzeszowski, W., Więcek, W., Kamiński, P. (2012). *Ochrona infrastruktury krytycznej*. Warsaw: AON, pp. 9-18.
12. Liedel, K. (2013). *Zwalczanie terroryzmu lotniczego: aspekty prawnomiędzynarodowe*. Warsaw: Jurysta, pp. 12-14.
13. Moteff, J.D. (2015). *Critical Infrastructures: Background, Policy, and Implementation*. Congressional Research Service, pp. 73-77.
14. *Narodowy Program Ochrony Infrastruktury Krytycznej* (2013). Available at: https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej, 20 October 2024.

15. Piątek, Z., Truchan J.R. (2013). *Technologie w ochronie infrastruktury krytycznej zewnętrznego kraju Unii Europejskiej.* Warsaw: Stowarzyszenie Ruch Wspólnot Obronnych, pp. 13-15.
16. Presch-Cronin, K., Marion, N.E. (2016). *Critical infrastructure protection, risk management, and resilience: a policy perspective.* CRC Press, p. 86.
17. *Terroryzm*. Available at: https://www.sjp.pwn.pl/szukaj/terroryzm.html, 20 October 2024.
18. Tyburska, A. (2010). Infrastruktura krytyczna – kluczowe problemy oraz strategiczne kierunki działań. In: Z. Piątek, A. Letkiewicz (eds.), *Terroryzm a infrastruktura krytyczna państwa – zewnętrznego kraju Unii Europejskiej.* Warsaw: Stowarzyszenie Ruch Wspólnot Obronnych, pp. 13-23.
19. Zabłocki, E. (ed.) (2009). Ochrona przed zagrożeniami terroryzmu lotniczego, Temat 2 (II.3.11.1.0). Warsaw: AON, pp. 19-27.