

Karol GEPPERT

31st Tactical Air Base Poznań-Krzesiny
ORCID: 0009-0007-4855-8248

DOI : 10.14746/ps.2023.1.16

Jerzy KONIECZNY

Adam Mickiewicz University, Poznań, Poland
ORCID: 0000-0002-9254-9134

ANALYSIS OF POTENTIAL THREATS TO THE CRITICAL INFRASTRUCTURE OF THE 31ST TACTICAL AIR BASE, IN THE CONTEXT OF THE SECURITY OF THE POZNAN AGGLOMERATION

INTRODUCTION

The determinants of our country's security environment are inextricably linked to changes of a political, economic, military or economic nature that are taking place in the international arena, over the past three decades, both on a European and global scale. The bipolar security system that took shape in the second half of the 20th century was an indicator of a bipolar system based on two political and military powers, the US and the USSR. However, with the collapse of communism or the Eastern Bloc, the disintegration of the Warsaw Pact and the regaining of independence by many nations, internal and external determinants changed, which began to shape Poland's new goals and interests.

In view of last year's aggression of the Russian Federation against Ukraine, as well as the continuation of actions on the part of Russia of a hybrid and asymmetric nature, and the mass movement of the population, we can speak of determinants that largely prevent the realization of national interests and the realization of strategic goals that are a guarantee of the security of our country. The likely effects of the threat in the face of multifaceted actions of a non-military, military or terrorist nature, can play a significant role in ensuring security, which we can define not only as a state, but also as a process that allows a sense of non-threat, stable existence and the possibility of development of all aggregated entities.

Today's geopolitical conditions of our country's security issues unequivocally indicate that one of the most important types of security of an object nature is military security. In definitional terms, military security is expressed as a state that is achieved as a result of the disposition of optimally organized and possessed by the Armed Forces of the Republic of Poland of adequate forces and means, allowing the realization of objectives, consistent with the interests of the strategic concept of the state (Wojnarowski, Babula, 2004: 13). The functioning of military units, which are organizational

units of the Armed Forces of the Republic of Poland, operating on the basis of the ethos assigned by the Minister of Defense (Dz. U. 2022, poz. 655), depends on the assigned tasks they are to carry out using the technical equipment and infrastructure they have on their equipment. In order for military units to perform their tasks properly and as intended, the priority is to protect and defend military facilities, which include military equipment, armaments and military critical infrastructure. Over several decades, the construction and location of military units, especially military airfields with their infrastructure and administrative and barracks buildings, took place outside the administrative boundaries of large urbanized zones. In an era of increasing population migration from outlying areas and the settlement of large urban areas, there has been rapid development of large urban areas, which has significantly contributed to changes in the spatial structure, as well as reducing the distances between military and civilian buildings.

The purpose of this paper is to define and identify potential factors that could pose a threat to both military critical infrastructure and the critical infrastructure of an urban agglomeration. The authors' intention is also an attempt to characterize several fundamental issues, in terms of analyzing hypothetical threats to military critical infrastructure, using the example of the 31st Tactical Air Base in Poznań, in the context of the security of the Poznań agglomeration.

CRITICAL INFRASTRUCTURE OF A MILITARY AIRPORT – DEFINITIONAL APPROACH

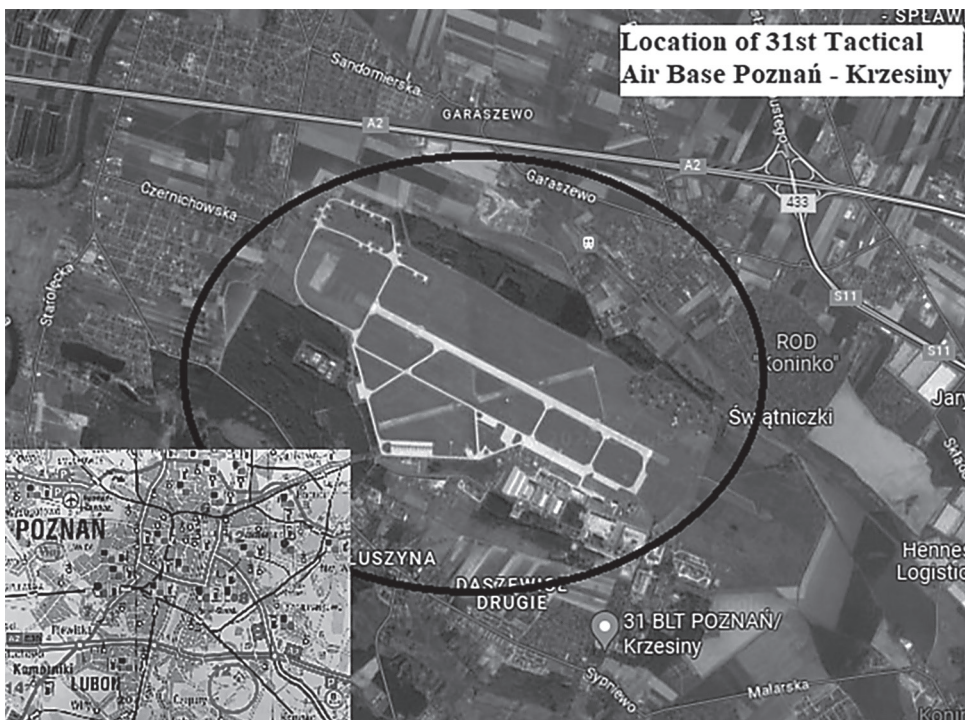
When considering the concept of critical infrastructure in the light of national normative documents, it should be understood as systems and their constituent functional interconnected facilities, equipment, installations and key services that serve to ensure the safe and efficient functioning of public administration bodies, as well as institutions and businesses (Dz. U. 2007, poz. 209, 1566 ze zm.). In the case of the definitional treatment of military critical infrastructure or critical infrastructure of a military airport, it should be assumed that these are elements of the state defense infrastructure, which includes facilities and equipment necessary for the performance of tasks, through organizational units subordinated to the Minister of Defense, and which form the basis for the proper process of functioning of the state defense system (*Słownik*, 2008: 53). It is worth noting that, in the face of military operations beyond our eastern border, the strategic objectives enshrined in the current National Security Strategy, which concern the multifaceted security of state organs and critical infrastructure, in response to increasing actions of an asymmetric, hybrid nature, as well as the increased activity of foreign intelligence services, both in the military and civilian spheres, take on particular importance (*Strategia*, 2020: 16).

As a result of the interpretation of the above definitional provisions, we will characterize the critical infrastructure of a military airport as elements of defense infrastructure, the operation of which must be preserved, in order to ensure broadly understood security and the performance of tasks in times of peace, crisis and war (Grenda, 2018: 5). The correctness of this definitional treatment of the critical infrastructure of a military airport,

is reflected in the description of a military airfield, in the Aviation Regulations of the Armed Forces of the Republic of Poland, which characterizes it as an airfield in use by the Ministry of National Defense for purposes related to national defense and security, and as a shared-use airfield, located on land owned by the state, under the permanent management of organizational units subordinate to the Minister of Defense, and entered in the register of airfields and military airfields (Grenda, 2019: 12).

The 31st Tactical Air Base is located in the southeastern part of the urban agglomeration and, as can be seen in the graphic below, is a surface facility that contrasts with its surroundings.

Figure 1. Location of 31st Tactical Air Base Poznań-Krzesiny



Source: Own study.

As can be seen, the military airport is characterized by a number of features that, due to its deployment, mode of activity, and regularity and repetition of operations, determine the following factors that allow its identification:

- location of the runway, taxiways and aircraft parking planes;
- location of fortified aircraft equipment centering areas with characteristic shelter – hangar buildings;
- location of lighting equipment, navigation systems, precision approach radars, combat agent depots, bomb depots;
- Airport Tower, barracks – administrative and hangar buildings with maintenance equipment (Grenda, 2019: 17).

The totality of point and linear objects characterized by their specific purpose and location on the territory of a military airfield and in its surroundings, results in easy identification and determines the potential threat from enemy actions and provides an opportunity to threaten the critical infrastructure of a military airfield.

CRITICAL INFRASTRUCTURE ELEMENTS 31ST TACTICAL AIR BASE

Analyzing the elements of the critical infrastructure of a military airport using the example of the 31st Tactical Air Base, we will characterize it as a number of facilities, equipment and resources performing specific tasks and services that enable the operation and continuity of training, logistics, as well as combat processes in accordance with its purpose. Using the example of the 31st Tactical Air Base, we can classify them into particular groups:

- surface objects – runway, taxiways and aircraft parking planes;
- point and line facilities – Air Traffic Control, shelters, hangars and buildings, storage facilities;
- data and communication service facilities.

In order to ensure the proper principles of operation and maintain an adequate level of security in the execution of tasks at the military airport Poznań-Krzesiny, we distinguish the following elements of critical infrastructure:

- runway – with a length of 2.5 km with a paved surface;
- aircraft staging planes allowing the dislocation of about 60 aircraft;
- an air traffic control tower to ensure safety for air traffic on the airport's maneuvering field and in the area surrounding the military airport;
- fortified aircraft dispersal areas with shelter-hangar buildings, allowing the dislocation of aircraft;
- storage facilities for propellants and lubricants included in the infrastructure consisting of underground storage tanks, stationary fuel stations and storage areas for storing and storing liquid fuels, oils and lubricants by type, including special fuel H-70;
- storage facilities for missiles, bombs and ammunitions;
- communications infrastructure and flight insurance e.g.:
 - stationery set TACAN (*Tactical Air Navigation*),
 - radiolocation set GCA (*Ground Control Approach*),
 - radio navigation system ILS (*Instrumental Landing System*);
- electro – light system CALVERT (*Cross Bar Approach Lighting System*);
- Airport Fire Department facilities;
- barracks and administrative buildings;
- security and defense facilities of the military air base.

All of the aforementioned elements of military critical infrastructure, their reliability and maintenance, are the basis for the safe and efficient operation of the air base. The probability of the occurrence of any threats, causing a disruption in their functioning may cause potential consequences affecting the security of military critical infrastructure, as well as the urban agglomeration in close proximity to it.

HAZARD CLASSIFICATION FOR A MILITARY AIRPORT

The term “threat” is formulated as “a situation or condition that threatens someone or in which someone feels threatened, or someone who creates such a situation.” (Drabik, Kubiak-Sokół, Sobol, 2006: 1215). In the case of military critical infrastructure, their security, stability and functionality of operation are crucial, so any potential threat can create danger and negatively affect, all processes related to its system (Milewski, 2016: 108).

For the purpose of this study, the author, proposed the following typology of threats to the military critical infrastructure of a military airport:

- military threats;
- non-military threats;
- asymmetric threats.

Technological development, widespread globalization and ongoing armed conflicts make us realize that the nature of threats is permanently evolving, and their identification is a continuous process and determines and verifies the developed assumptions, related to the protection of military critical infrastructure.

A classic example of the use of military capabilities, with the aim of neutralizing and disabling the operational capability of military airfields, is the example of the air strike against targets in Egypt, Jordan and Syria during Operation Focus during the 1967 Israeli-Arab War, during which 11 airfields located in the Sinai Peninsula and within Egypt were destroyed in an airstrike of only a few minutes by the Israeli Air Force. During the course of an armed conflict, the Armed Forces’ operations are aimed at eliminating and neutralizing the enemy’s defensive capabilities and forces and means used in the airspace, as well as in the telecommunications zone and the critical infrastructure of the military airport. Diversification of actions taken, in order to disrupt the critical infrastructure system and eliminate military potential, can be characterized by the following elements:

- attack from the air using their own resources of aircraft, helicopters with available armaments, but also as indicated by ongoing operations on the modern battlefield, using the example of the Nagorno-Karabakh conflict or the fighting between Israel and Palestine using armed drones;
- as well as by conducting artillery or rocket fire, as part of the neutralization and deprivation of functional and operational capability of military critical infrastructure systems of a military airport (Grenda, 2018: 12).

In terms of non-military threats, it is necessary to distinguish, first of all, threats related to natural and technical hazards (Dz. U. 2014, nr 62, poz. 333 i 915 ze zm.):

- floods;
- fires;
- strong winds;
- technical accidents or traffic collisions resulting from human activity, in particular, during the transportation of hazardous materials, aerial warfare agents or aviation fuel.

Some of the most unpredictable threats that can occur in the area of a military airport and directly pose a danger to military critical infrastructure are any actions

of an asymmetric and hybrid nature. It should be noted that the actions taken can occur both during peace, crisis and during regular military operations. Very often, they are characterized by the use of synchronized unconventional measures aimed at exploiting gaps in the system of defense and protection of military facilities, and by achieving a synergistic effect, can simultaneously affect the public mood of the civilian population living in close proximity to a military airport. Any activities undertaken with asymmetric or hybrid characteristics, are defined as activities below the threshold of war and are often initiated by non-state actors. In the case of the occurrence of asymmetric threats, in view of the security of the military critical infrastructure of a military airport, we can distinguish the following division of them:

- the threat of a terrorist attack;
- the threat of an attack of a cyber nature;
- acts of sabotage or criminal in nature;
- unauthorized entry;
- unauthorized landing of an aircraft.

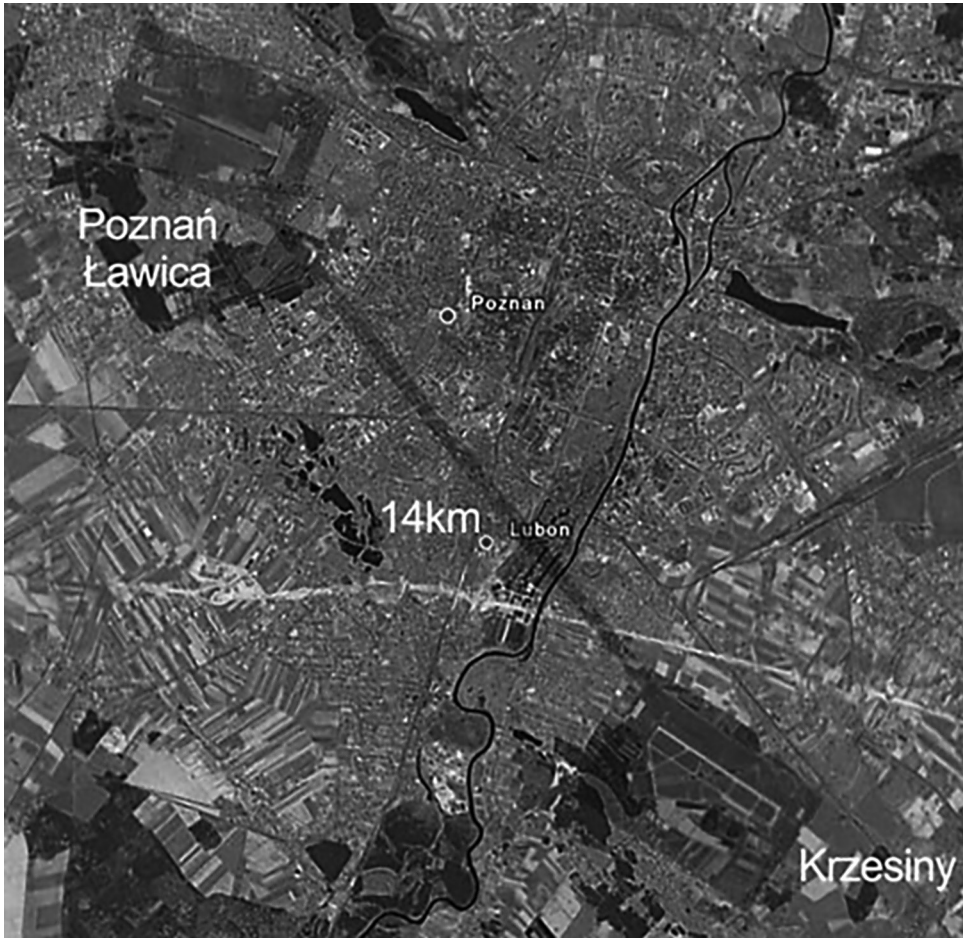
The consequences of the terrorist attacks we have witnessed in the last two decades, the actions of mercenaries and organized crime groups, or the diversification of military activities during Russia's aggression against Ukraine, clearly indicate that the developed system models for the protection and defense of military facilities are not a closed process, but should be considered in terms of permanent modernization. The above proposed typology of threats to military critical infrastructure, and, in particular, threats of asymmetric and hybrid nature, clearly indicate that in the era of today's situation in Ukraine and the ongoing fighting across our eastern border, indicate that the probability of their occurrence increases dramatically, which can result in a real threat to the infrastructure of a military airport, but also to the urban agglomeration in its close vicinity.

EXAMPLES OF EXISTING THREATS TO INFRASTRUCTURE CRITICAL INFRASTRUCTURE OF A MILITARY AIRPORT

One of the most serious examples of threats to the critical infrastructure of a military airport at the 31st Tactical Air Base, occurred on August 16, 2006, and was related to the unauthorized landing of a passenger aircraft of Boeing 737-400 of Turkish SKY Airlines with 170 passengers on board, at Poznań-Krzesiny military airport. According to the Final Report of the State Commission for Investigation of Aviation Accidents No. 245/06, "The flight was performed in accordance with instrument flight rules (IFR)." The crew of SHY335 established radio communication with the air traffic control authority of Poznań-Ławica Airport (TWR EPPO) and received permission to execute the airport approach procedure under IFR – ILS/DME "Y" RWY29. After performing a touchdown and reporting his position "FINAL" to the EPPO TWR, he received permission to land on EPPO RWY29. After a few minutes of flight, as a result of misidentification of the airport, SHY335 landed without permission from the appropriate air traffic service authorities at Poznań-Krzesiny

Military Airport (EPKS) located at a distance of 13.8 km (7.4 NM) southeast of the EPPO.” (*Raport*, 2007: 4).

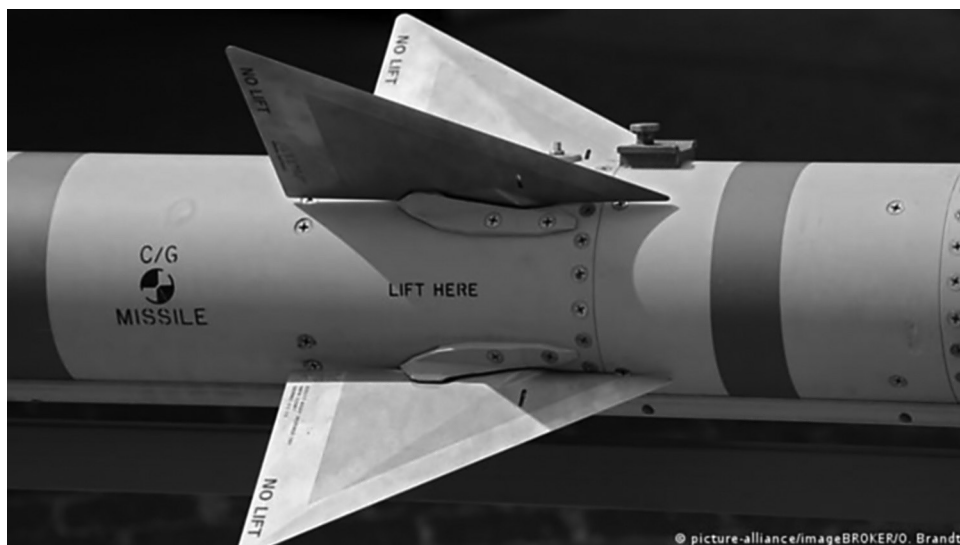
Figure 2. Location of 31st Tactical Air Base Poznań-Krzesiny and civil airport Poznań-Lawica



Source: Cybulak, Kalinowska, 2006.

Another example of a potential threat to critical infrastructure, both civilian and military, was an incident that occurred on September 10, 2020, during a routine training flight to the Nadarzyce training ground. One of the aircraft, belonging to the 31st Tactical Air Base took off from the airport in Krzesiny and headed for the training ground in Nadarzyce, and while continuing the flight, a metal element became detached from the aircraft, or more precisely from the suspended training armament, and fell onto a private property located in Luboń near Poznań. As a result of contact with the ground, the object traveled and hit a private passenger car standing on the property, damaging it.

Figure 3. Example of armament – medium-range air-to-air missile
AIM-120 AMRAAM



Source: Deutsche Welle, 2020.

The examples of incidents described above, indicate the possibility of a variety of threats that can threaten the military critical infrastructure of a military airport, as well as the infrastructure of an urban agglomeration.

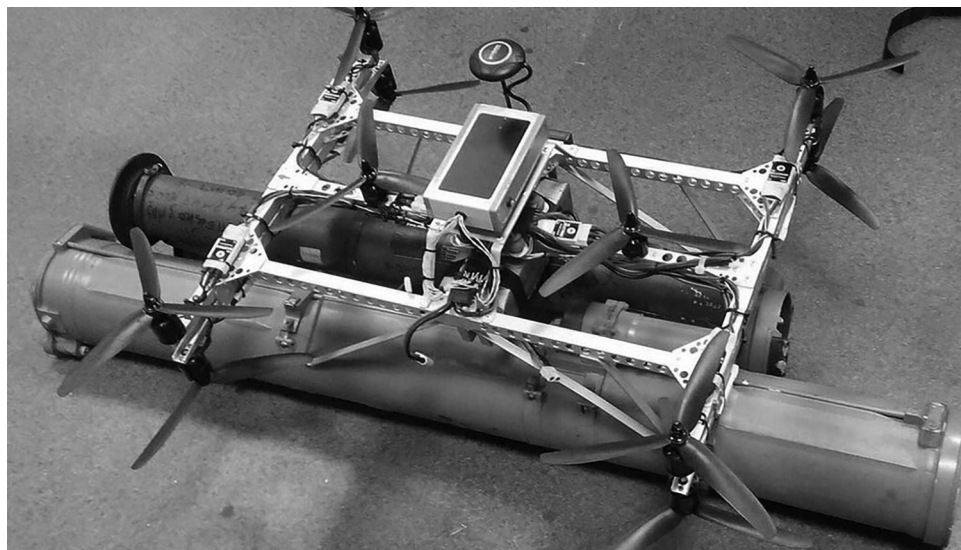
EXAMPLES OF POSSIBLE THREATS TO THE CRITICAL INFRASTRUCTURE OF A MILITARY AIRPORT

In the dynamically changing geopolitical situation in the world and analyzing military operations during the armed conflict in Ukraine, we conclude that the elimination and prevention of operational activities, using military airfields, is an extremely important factor on the modern battlefield. It will have the effect of lowering the combat capability of the opponent, as well as enabling the maintenance of combat capability and creating favorable conditions for tactical operations and providing freedom to conduct tactical operations by own troops (*Regulamin*, 2008: 17). The military critical infrastructure of a military airport plays a key role in ensuring the continuity of the process of securing flight training, and will therefore be one of the main targets of an adversary's influence. However, it should be borne in mind that the undertaking of activities related to the exclusion of the functionality of a military airfield, may occur during peace, crisis or war (Grenda, 2019: 7). Analyzing the Russian-led military operation in Ukraine, in its initial phase, Russian troops focused their actions on neutralizing civilian and military infrastructure, in particular targeting the bombing of Ukrainian military airfields. However, it needs to be emphasized that the asymmetric and hybrid actions undertaken can be carried out by both states and any non-state ac-

tors, who in many cases use unconventional means of the specific nature of the means they use (Ciekanowski, 2009: 52).

Over the past few years, in an era of technological advances, as well as low cost and virtually unlimited acquisition possibilities, so-called UAVs (Unmanned Aerial Vehicle) have become a very popular tool in the hands of criminals, terrorists or mercenaries. Popular drones, which undergo modifications for the needs of various entities and are adapted to carry improvised explosive devices or warfare agents. The operator of the device, due to the variety of available designs and the ability to program and control the drone over long distances, can carry payloads properly built on the device and remotely initiate their detonation, in close proximity to elements of the military critical infrastructure of a military airport.

Figure 4. An example of a modified drone prepared to carry anti-tank missile launchers



Source: Marszałkiewicz, 2017: 3.

How dangerous as well as inexpensive these weapons can be is evidenced by examples of their real-world use near military units, elements of critical infrastructure, and the use of such devices, during the armed conflict in Ukraine.

In March 2014, on the main apron of the airport of the 8th Transport Aviation Base in Krakow, an unidentified operator dropped an explosive device using a drone, which detonated, and the perpetrator, within the scope of his act, committed a violation of aviation law and the introduction of a danger of a catastrophe in air traffic. As a result of the investigation conducted by the Appellate Prosecutor's Office in Krakow and the Internal Security Agency, it was established on the basis of footage that a flare was dropped from the drone, and investigators confirmed that it could have caused a danger to the aircraft (Newsweek, 2015).

In December 2022, a drone armed with an explosive device destroyed a fuel tank at a military airfield in Kursk, Russia. A drone explosion at Engels air base near Saratov

damaged two Russian Tu-95 bombers, while a fuel truck exploded at Diaghilevo air base in Ryazan. The Ukrainian side has not officially confirmed its connection to these events.

In February 2023, two drones penetrated a military airfield in Machulishchi, Belarus, causing damage to a Beriyev aircraft, AEWAC (Airborne Early Warning And Control) A-50 of the Air and Space Forces of the Russian Federation.

Figure 5. Satellite images of the A-50 aircraft at the airport in Machulisky, Belarus



Source: Militarnyi – Organizacja..., 2023.

Widespread globalization, and before all, mass migration forced by military action in Ukraine, is causing frequent population movements, both in improving economic conditions, but also as a result of saving their own lives. One of the dilemmas, due to operations under time pressure, during the evacuation of the population from occupied or war zones, is the procedure for detailed identification of individual migrants or refugees. The situation, increases the risk of violations of their rights and freedoms, which can result in negative discriminatory phenomena and influence the desire to take retaliatory or criminal actions, but also allows the movement of people who have been punished or are suspected of having committed crimes.

The above conditions, may contribute to the infiltration of individuals, potentially interested in undertaking diversionary activities, into groups or associations that bring together people interested in aviation in their ranks, through membership in spotters' groups. Spotters generally combine their love of aviation and aircraft themselves with simultaneous photography of flying objects. They very often occupy positions under the fences of airports or on the approach paths of aircraft landings.

Another likely factor that could pose a threat to the military critical infrastructure of a military airport, but also pose a danger to aircraft, could be the use of mobile missile kits. At the current time, when the ongoing armed conflicts are influenced by

the intensification of international trade in various types of armaments, as well as the availability, mobility and low cost of acquisition, this may be an alternative to achieve certain objectives by various actors, with a relatively measurable cost-effectiveness relationship. The modern battlefield and the type of operations carried out by the warring parties, point to the ever-increasing needs, in terms of acquiring an effective and low-cost type of armament, which, as evidenced by the observation of the ongoing conflict in Ukraine, can be effective, uncomplicated to use, does not require large logistical outlay and transportation, and is easy to mask. The growing arms trade, the scale of the ongoing conflicts and their location on the world map mean that some of this type of weaponry, remains beyond the control not only of the states that produce the portable weapons sets, but also by their buyers, including non-state actors and groups of a terrorist nature (Compa, 2018: 104).

Russian sets “Arrow-2”, American sets of the “Stinger” type, missile set of Polish production “Piorun”, or portable anti-aircraft missile set of the 4th generation of Turkish production “Sungur”, can pose a real threat to aircraft operating from the military airport, as a result of the use of this type of armament, by terrorist individuals or groups. As the activities of Ukraine’s regular armed forces, but also of unidentified entities, indicate, the effectiveness of the use of portable rocket sets in combating enemy aircraft is very high. On February 13, in the evening at 18:03, a Su-24M frontline bomber was shot down, using the PPZR “Thunderbolt” launcher. The machine was hit by the first fired missile during, a bombing attack on Ukrainian positions in the Bakhmut area (Szopa, 2023). In May 2022, the Ukrainian side, confirmed the downing of a Russian Ka-52 Alligator attack helicopter in the Kharkiv region in eastern Ukraine, using the “Piorun” mobile missile kit. The above examples provide evidence that the potential use of portable missile sets, to disrupt elements of a military airport’s critical infrastructure, is highly likely.

The last determinant that can become a real threat to the safe operation of a military airport can be cyberattacks motivated by the desire to undermine the image of the organization in question and the effectiveness of its protection, but primarily to gain access and acquire strategic data, as well as to interfere with telecommunications systems, flight insurance systems and aircraft operations support systems. Analyses from the first half of 2022, by the Israeli company “Check Point Research,” which specializes in minimizing cyber threats and attacks, present data on documented attack attempts in the military-civilian sector in our country, at more than 1,100 per week (CPR, 2022).

The ability to use the Internet by individual hackers, cyber criminals or organized terrorist groups, is permanently improved and developed, and the possibility of minimizing the leaving of any traces of activity on the Internet, at very low cost and with little effort makes it one of the zones with the most important points of strategic perception of national defense, along with its elements of critical infrastructure (Leśnikowski, 2018). The most recognizable and technologically advanced step taken towards unauthorized intrusion into critical infrastructure installations was in late 2009 – early 2010, the use of a so-called computer worm called “Stuxnet” to spy on and reinstall the software of industrial installations, targeting a nuclear power plant in Iran. Microsoft’s recent 2022 report. “Defending Ukraine: Early Lessons from the Cyber War” states that Microsoft detected Russian hacking attempts at 128 organizations in

42 countries outside Ukraine. While the United States has been Russia's number one target, this activity has also prioritized Poland, where much of the logistical delivery of military and humanitarian aid is coordinated (*Raport*, 2022).

At the Air Base, as well as in the entire area of operations using ICT networks, data transmission, or aircraft operations support systems, all activity and server placement is carried out through internal and independent networks with limited access. However, this does not exclude the possibility of breaking through network security and interfering with systems and installations, related to the functionality of the military critical infrastructure of a military airport.

POTENTIAL CONSEQUENCES OF THE LACK OF RESILIENCE OF THE CRITICAL INFRASTRUCTURE OF THE 31ST TACTICAL AIR BASE FOR THE SECURITY OF POZNAŃ AGGLOMERATION

For a definition of critical infrastructure, see the Law of April 26, 2007 (Dz. U. 2007, nr 89, poz. 590) on crisis management, and is understood as systems and their constituent facilities functionally related to each other, and facilities and services that constitute the security of the state and its citizens, and serve to ensure the effective operation of state bodies, institutions and businesses. Systems included in the critical infrastructure, are defined in terms of their functionality as systems providing energy and fuel supply, communication systems and information and communication networks, financial systems, water and food supply, health care system, transportation and communication systems, rescue systems, ensuring the continuity of public administration, as well as those related to the production, storage, warehousing and use of chemical and radioactive substances, along with including pipelines of hazardous substances.

The security of the Poznań agglomeration with its thematic scope, includes very important aspects of the safety of its residents, especially in terms of its proper functioning. Located within the boundaries of the urban agglomeration, the military airport and the 31st Tactical Air Base operating on its territory, along with the along with intensively operated aviation equipment, interact positively on many levels, whether social, economic, service or educational, but can also be an object of interest, for the activities of individuals or groups of a criminal or terrorist nature. All of the previously mentioned examples of potential threats to the military infrastructure of a military airport, have been and are being addressed in times of peace, crisis and war. In the case of such a large agglomeration as the Poznań agglomeration and the elements located on its territory, statutorily defined in the resources of the systems included in the critical infrastructure, may be the target of activities of certain groups that, using the available means and methods to threaten the military airport infrastructure with aircraft, will want to achieve a synergistic effect and, at the same time, destabilizing the operational functionality of the military airport, threaten the critical infrastructure of the Poznań agglomeration and provoke certain public sentiments.

Analyzing the statutory provisions on systems containing elements of critical infrastructure, this study proposes selected facilities, located in the Poznań metropolitan area, and which may be a potential target for the impact of individuals or non-state ac-

tors, as a result of taking disorganization and destructive actions in the military critical infrastructure system of a military airport.

One of the most important surface facilities located on the territory of the city of Poznań, which is part of the critical infrastructure, is the Debina infiltration water intake, which is part of the Poznań Water Supply System. The Debina water intake, developed over a length of 3.2 km, is hydrogeologically located within the uncovered Quaternary groundwater reservoir of the Warta River valley, on a flood terrace about 1.1 km wide. It is an artificial infiltration intake, the main components of which are a river water pumping station, infiltration ponds (natural, primary, casing and lateral), intake wells and collection wells. Currently, the nominal capacity of the Debina intake is estimated at 72.900–78.800 m³/day (Bartosik, Chomici, 2010: 86).

Another potential facility that belongs to the strict critical infrastructure is Veolia Energia Poznań SA. Which produces system heat and electricity in cogeneration and manages the district heating network. It supplies about 60 percent of the city's population with heat, as well as industrial plants, public institutions and shopping and service centers (Veolia, 2023).

One of the largest industrial plants located in the Poznań agglomeration, is the chemical industry company Centrala Luvena S.A. in Luboń, which manufactures fertilizers, impregnants and pesticides (Luvena, 2023).

In terms of communication hubs, transportation hubs, container terminals and transshipment terminals, which can be an object of influence in terms of destabilizing critical infrastructure, is the Poznań Franowo Container Terminal. The terminal in Franowo is located at the intersection of two European transport corridors: East-West and North-South. The first connects to the New Silk Road, a rail link between China and Western Europe. The second connects the Baltic Sea to the Adriatic coast.

Threat from deliberate third-party action:

- terrorist or cyber-terrorist attack;
- interference with remote control elements;
- use of improvised explosive devices with explosives;
- attack by a psychopath or an act of vandalism.

Threat within the location:

- traffic accident;
- air plane crash;
- environmental pollution;
- lack of usability and functionality, caused by a land or air disaster;
- power, water, gas and district heating emergencies;
- release of toxic industrial agents, in the form of gases, liquids or solids;
- release of radioactive and biological materials;
- interruption of the supply chain;
- proximity to transportation hubs.

All of the facilities discussed above and proposed, may pose a potential threat to the Poznań agglomeration, due to the likelihood of disruption productive functionality and interference with security systems, as a result of intentional action on the part of unidentified entities, but also as a result of their activities in the area of elements of the military critical infrastructure system.

SUMMARY AND CONCLUSIONS

Armed conflicts, terrorist acts or asymmetric or hybrid activities undertaken, have become an integral part of our daily life. The effects of these activities, both direct and indirect, are always a determinant of the emergence of emergencies, but also reflect any inadequacies in the protection and defense and security systems, in terms of the functioning of critical infrastructure elements. The location of a military airfield with such a large area, which remains in the use of the 31st Tactical Air Base, in addition to the distribution of military infrastructure elements over a large area, makes ensuring the security of its operation a demanding process, and the disruption of some of its elements leads to disorganization and disrupts the functioning of other systems. In the case of the discussed and indicated potential threats, both to the security of the military airport and the security of the urban agglomeration, it should be presumed that the described phenomena will not materialize, but also require the development and continuous updating in view of the changing security environment, and system solutions at all levels of civil-military cooperation.

Taking measures to permanently improve security should focus on the implementation of tasks belonging only to the military and include activities related to the training of personnel responsible for the military airport security and defense system, as well as maintaining the technical condition of facilities and infrastructure elements at a level that ensures their effective operation. In terms of maintaining the cleanliness of airport surfaces and to prevent the penetration of so-called “drones” into the airport area, work on developing an early warning system and minimizing the effects of drones over the military airport area should be intensified. The training process should be enriched with a permanent element on topics related to related to cyber-security and the possibilities of minimizing attack attempts using ICT networks.

In the area of non-military operations, systems related to the related to the identification of individuals within a military airfield, with a particular focus on those who are not affiliated with formal groups or organizations related to spotting. Services related to intelligence and counterintelligence should continue to acquire, analyze and process the data and information obtained related to related to potential threats within critical infrastructure.

Cooperation between state and private entities, as well as between the Police, Military Police and internal security bodies, should continue and intensify, in view of the dynamic changes on the geopolitical scene in terms of information sharing, as well as the improvement of protective systems and based on the on the basis of uniformity of operational procedures.

REFERENCES

- Bartosik A., Chomicki I. (2010), *100 lat eksploatacji infiltracyjnego ujęcia wody Dębina w Poznaniu – czas na zmiany*, Poznań.
- Compa T. (2018), *Współczesne zagrożenia bezpieczeństwa transportu lotniczego*, WOSSIP, Dęblin.
- Ciekanowski Z. (2009), *Działania asymetryczne jako źródło zagrożeń bezpieczeństwa*, Warszawa.

- CPR – Check Point Research (2022), *Polska wśród najbardziej atakowanych przez hakerów krajów Europy. RAPORT*, <https://technologia.dziennik.pl/internet/artykuly/8480634,hakerzy-ataki-europa-check-point.html> (10.02.2023).
- Cybulak P., Kalinowska D. (2006), *Wylądowała 14 km od Ławicy...*, „Pasazer News”, 16 August, <https://www.pasazer.com/news/1549/wyladowala,14,km,od,lawicy.html> (01.02.2023).
- Deutsche Welle (2020), *Węgry kupią w USA broń za miliard. „Historyczny deal”*, <https://www.dw.com/pl/w%C4%99gry-kupi%C4%85-w-usa-bro%C5%84-za-miliard-dolar%C3%B3w-pok%C3%B3j-jest-teraz-bardzo-kruchy/a-54551112> (02.02.2023).
- Drabik L., Kubiak-Sokół A., Sobol E. (2006), *Słownik języka polskiego PWN*, Warszawa.
- Dron zrzucił ładunek wybuchowy na lotnisko w Balicach? ABW prowadzi śledztwo* (2015), „Newsweek”, 23 July, <https://www.newsweek.pl/polska/dron-nad-lotniskiem-w-balicach-czy-zrzucil-ladunek-wybuchowy/1y6fs19> (04.02.2023).
- Grenda B. (2018), *Zagrożenia asymetryczne militarnej infrastruktury krytycznej*, „Przegląd Policyjny”, No. 4/132, Szczytno.
- Grenda B. (2019), *Bezpieczeństwo lotnisk wojskowych*, Wydawnictwo Silva Rerum, Poznań.
- Leśnikowski W. (2018), *Cyberataki na infrastrukturę krytyczną jako tanie i skuteczne środki do paraliżowania rozwiniętych państw*, Bydgoszcz.
- Luvna (2023), <https://luvena.pl/aktualnosci/> (18.02.2023).
- Marszałkiewicz Z. (2017), *Zagrożenie dla portów lotniczych ze strony bezzałogowych statków powietrznych*, „Przegląd Komunikacyjny”, No. 12, Gdańsk.
- Milewski J. (2016), *Identyfikacja infrastruktury krytycznej i jej zagrożeń*, Akademia Sztuki Wojennej, Warszawa.
- Militarni – Organizacja społeczna Ukrainie Centrum Militarne (2023), *Opublikowano pierwsze zdjęcia satelitarne rosyjskiego samolotu A-50 po ataku*, <https://mil.in.ua/pl/news/opublikowano-pierwsze-zdjecia-satelitarne-rosyjskiego-samolotu-a-50-po-ataku/> (07.02.2023).
- Newsweek (2015), *Dron zrzucił ładunek wybuchowy na lotnisko w Balicach? ABW prowadzi śledztwo*, <https://www.newsweek.pl/polska/dron-nad-lotniskiem-w-balicach-czy-zrzucil-ladunek-wybuchowy/1y6fs19> (04.02.2023).
- Opublikowano pierwsze zdjęcia satelitarne rosyjskiego samolotu A-50 po ataku* (2023), „Militarny”, 23 February, <https://mil.in.ua/pl/news/opublikowano-pierwsze-zdjecia-satelitarne-rosyjskiego-samolotu-a-50-po-ataku/> (07.02.2023).
- Raport Defending Ukraine: Early Lessons from the Cyber War* (2022).
- Raport Końcowy Państwowej Komisji Badania Wypadków Lotniczych, Nieautoryzowane lądowanie na lotnisku wojskowym Poznań-Krzesiny (EPKS) samolotu Boeing 737-400 w dniu 16 sierpnia 2006 roku, Poważny incydent nr: 245/06* (2007), Warszawa.
- Raport NIK Informacja o wynikach kontroli przygotowania lotniska w Poznaniu-Krzesinach do bazowania samolotów F-16 nr ewid. 147/2011/P09/084/KOB* (2011), Warszawa.
- Regulamin działań Wojsk Lądowych* (2008), Warszawa.
- Regulamin Lotów Lotnictwa Sił Zbrojnych RP* (2016), Warszawa.
- Russian Ordnance Group Adapts Grenade Launchers to Arm Drone* (2018), „Defense Update”, 5 October, <https://defense-update.com/20181005.html> (02.02.2023).
- Słownik terminów z zakresu bezpieczeństwa narodowego* (2008), Warszawa.
- Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* (2020), Warszawa.
- Szopa M. (2023), *Są zdjęcia satelitarne. Jak wyglądają uszkodzenia rosyjskiego samolotu dowodzenia?*, „Defence-24”, 1 March, <https://defence24.pl/sily-zbrojne/sa-zdjecia-satelitarne-jak-wygladaja-uszkodzenia-rosyjskiego-samolotu-dowodzenia> (10.02.2023).

- Ustawa o przebudowie i modernizacji technicznej oraz finansowaniu Sił Zbrojnych Rzeczypospolitej Polskiej w latach 2001–2006* (2001), Dz. U. 2009, nr 67, poz. 570 ze zm.
- Ustawa o ustanowieniu programu wieloletniego „Wyposażenie Sił Zbrojnych Rzeczypospolitej Polskiej w samoloty wielozadaniowe” i zapewnienia warunków jego realizacji* (2001), Dz. U. 2001, nr 89, poz. 972 ze zm.
- Ustawa o stanie klęski żywiołowej* (2002), Dz. U. 2014, nr 62, poz. 333 i 915 ze zm.
- Ustawa o zarządzaniu kryzysowym* (2007), Dz. U. 2007, nr 89, poz. 590.
- Ustawa o obronie Ojczyzny* (2022), Dz. U. 2022, poz. 655.
- Veolia* (2023), <https://energiadlapoznania.pl/o-nas/> (19.02.2023).
- Węgry kupią w USA broń za miliard dolarów. „Pokój jest teraz bardzo kruchy”* (2020), “Deutsche Welle”, 13 August, www.dw.com/pl/w%C4%99gry-kupi%C4%85-w-usa-bro%C5%84-za-miliard-dolar%C3%B3w-pok%C3%B3j-jest-teraz-bardzo-kruchy/a-54551112 (02.02.2023).
- Wojnarowski J., Babula J. (2004), *Bezpieczeństwo militarne Rzeczypospolitej Polskiej*, AON, Warszawa.

ABSTRACT

The main purpose of the article is an attempt to analyze the potential threats to the critical infrastructure of the 31st Tactical Air Base in Poznań-Krzesiny in terms of the security of the Poznań agglomeration. The main threats that may occur have been indicated in the context of military, non-military, asymmetric or hybrid activities. In addition, the mortgage effects of the actions taken, which can have a measurable impact on the safety of the Poznań agglomeration, were discussed and presented. An additional thread in the article is the indication of the existing threats that took place in the area of the Poznań-Krzesiny military airport, which could threaten the functioning of the critical infrastructure located in the area of the 31st Tactical Air Base and the critical infrastructure located in the area of the Poznań agglomeration.

The article does not contain any information or data defined as classified information in accordance with Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.

Keywords: critical infrastructure, military airport, threat, security, urban agglomeration, Air Base, Armed Forces

ANALIZA POTENCJALNYCH ZAGROŻEŃ INFRASTRUKTURY KRYTYCZNEJ 31 BAZY LOTNICTWA TAKTYCZNEGO, W KONTEKŚCIE BEZPIECZEŃSTWA AGLOMERACJI POZNAŃSKIEJ

STRESZCZENIE

Głównym celem artykułu jest próba analizy potencjalnych zagrożeń infrastruktury krytycznej 31. Bazy Lotnictwa Taktycznego w Poznaniu-Krzesinach w aspekcie bezpieczeństwa aglomeracji poznańskiej. Wskazano główne zagrożenia mogące wystąpić w kontekście podjęcia działań o charakterze militarnym, niemilitarnym, a także o charakterze asymetrycznym lub hybrydowym. Ponadto omówiono i przedstawiono hipotetyczne skutki podejmowanych działań, które w wymierny sposób mogą wpłynąć na bezpieczeństwo aglomeracji poznańskiej. Dodatkowym wątkiem w artykule jest wskazanie zaistniałych zagrożeń, jakie miały miejsce w rejonie lotniska wojskowego Poznań-Krzesiny, a które mogły zagrażać funkcjonowaniu infrastruktury

krytycznej zlokalizowanej na terenie 31. Bazy Lotnictwa Taktycznego oraz infrastruktury krytycznej znajdującej się w obszarze aglomeracji Poznańskiej.

W artykule nie umieszczono żadnych informacji ani danych definiowanych jako informacja niejawna, zgodnie z Ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.

Słowa kluczowe: infrastruktura krytyczna, lotnisko wojskowe, zagrożenie, bezpieczeństwo, aglomeracja miejska, Baza Lotnicza, Siły Zbrojne

