Studia Bezpieczeństwa Narodowego
Zeszyt 38 (2025)
ISSN 2028-2677, s. 49-68
DOI: 10.37055/sbn/218069

Instytut Bezpieczeństwa
Wydział Bezpieczeństwa, Logistyki i Zarządzania
Wojskowa Akademia Techniczna
w Warszawie

National Security Studies
Volume 38 (2025)
ISSN 2028-2677, pp. 49-68
DOI: 10.37055/sbn/218069

Institute of Security
Faculty of Security, Logistics and Management
Military University of Technology
in Warsaw

A MULTILAYERED SECURITY ARCHITECTURE OF MILITARY AIRBASES UNDER HYBRID THREAT CONDITIONS

WIELOWARSTWOWA ARCHITEKTURA BEZPIECZEŃSTWA WOJSKOWYCH LOTNISK W WARUNKACH ZAGROŻEŃ HYBRYDOWYCH

Adam RURAK
Polish Air Force University in Dęblin
ORCID: 0000-0002-5842-8048

Abstract. This article addresses the security of military airbases as critical elements of national defence systems operating in an increasingly complex environment of hybrid and asymmetric threats. Contemporary threat landscapes, shaped by the proliferation of unmanned aerial systems, cyber operations, sabotage, and irregular tactics, challenge traditional, perimeter-focused models of airbase protection and expose structural vulnerabilities in dispersed and spatially extensive military infrastructure. The aim of the study is to conceptualise and analyse a multilayered security architecture for military airbases operating under contemporary hybrid threat conditions, with particular emphasis on its legal, organizational, technical, and planning dimensions. The central research problem concerns the extent to which existing legal, organizational, technical, and procedural arrangements are adequate to ensure the operational continuity and resilience of military aviation facilities in both peacetime and crisis conditions. The article advances the hypothesis that effective military airbase security cannot be reduced to isolated technological solutions but depends on the coherent integration of multilayered protective systems encompassing legal mandates, organizational responsibilities, physical and technical safeguards, and appropriately trained personnel within a unified planning framework. On the basis of a narrative review of NATO doctrinal documents, Polish Armed Forces regulations, and relevant academic literature published between 2000 and 2023, the analysis examines five interrelated domains of airbase protection: legal and organizational frameworks, physical protection systems, technical security measures, zonal defence architecture, and planning and risk management processes. The findings indicate that, despite extensive use of fencing, access control, surveillance technologies, and guard forces, significant vulnerabilities persist, particularly with regard to low-cost UAV incursions, cyber disruptions, insider threats, and asymmetric attacks targeting dispersed infrastructure components. The study underscores the importance of adaptive planning, continuous risk assessment, and interoperability among military units, law enforcement agencies, and contracted security providers. By proposing a holistic and practice-oriented framework for military airbase protection, the article

contributes to ongoing national and NATO-level debates on safeguarding critical defence infrastructure and highlights the necessity of a system-based approach to airbase security in an evolving threat environment.
Abstrakt. Artykuł podejmuje problematykę bezpieczeństwa lotnisk wojskowych jako kluczowych elementów systemów obrony państwa funkcjonujących w warunkach narastających zagrożeń hybrydowych i asymetrycznych. Współczesne środowisko bezpieczeństwa, kształtowane przez proliferację bezzałogowych statków powietrznych, operacje cybernetyczne, działania sabotażowe oraz taktyki nieregularne, podważa tradycyjne, perymetryczne modele ochrony infrastruktury lotniczej i ujawnia systemowe podatności rozległych, przestrzennie rozproszonych obiektów wojskowych. Celem pracy jest konceptualizacja oraz analiza wielowarstwowej architektury bezpieczeństwa wojskowych lotnisk funkcjonujących w warunkach współczesnych zagrożeń hybrydowych, ze szczególnym uwzględnieniem jej prawnych, organizacyjnych, technicznych oraz planistycznych wymiarów. Główny problem badawczy dotyczy adekwatności obowiązujących rozwiązań prawnych, organizacyjnych, technicznych i proceduralnych w zapewnianiu ciągłości funkcjonowania oraz odporności lotnisk wojskowych zarówno w czasie pokoju, jak i w sytuacjach kryzysowych. W pracy przyjęto hipotezę, że skuteczność bezpieczeństwa lotnisk wojskowych nie wynika z zastosowania wyizolowanych środków technologicznych, lecz z integracji wielowarstwowych systemów ochrony obejmujących normy prawne, struktury organizacyjne, zabezpieczenia techniczne oraz odpowiednio przygotowany personel, funkcjonujące w ramach spójnych procesów planistycznych i zarządzania ryzykiem. Analiza została oparta na narracyjnym przeglądzie źródeł doktrynalnych, prawnych, organizacyjnych i technicznych, w tym dokumentów NATO, regulacji Sił Zbrojnych RP oraz literatury naukowej opublikowanej w latach 2000–2023, ze szczególnym uwzględnieniem pięciu powiązanych obszarów: ram prawno-organizacyjnych, systemów ochrony fizycznej, technicznych środków bezpieczeństwa, architektury ochrony strefowej oraz procesów planowania i zarządzania ryzykiem. Wyniki wskazują, że pomimo stosowania rozbudowanych systemów ogrodzeń, kontroli dostępu, technologii nadzoru oraz stałej obecności służb ochrony, utrzymują się istotne podatności, zwłaszcza w zakresie niskokosztowych naruszeń z użyciem BSP, zagrożeń cybernetycznych, zagrożeń wewnętrznych oraz ataków asymetrycznych wymierzonych w rozproszoną infrastrukturę. Podkreślono znaczenie adaptacyjnego planowania, ciągłej oceny ryzyka oraz interoperacyjności pomiędzy jednostkami wojskowymi, organami ścigania i podmiotami ochrony kontraktowej. Zaproponowane w artykule holistyczne i zorientowane na praktykę ramy ochrony lotnisk wojskowych stanowią wkład do krajowych i natowskich debat dotyczących zabezpieczania krytycznej infrastruktury obronnej oraz potwierdzają konieczność systemowego podejścia do bezpieczeństwa w dynamicznie zmieniającym się środowisku zagrożeń.
Keywords: hybrid threats; military infrastructure; NATO; defence-in-depth; critical infrastructure protection.
Słowa kluczowe: zagrożenia hybrydowe; infrastruktura wojskowa; NATO; obrona warstwowa; ochrona infrastruktury krytycznej.

Introduction

Military airbases constitute complex and spatially dispersed socio-technical systems whose operational continuity depends on the integration of multiple protective layers. In contemporary security environments shaped by hybrid threats, including unmanned aerial systems, cyber operations, sabotage and asymmetric tactics, traditional perimeter-focused protection models are increasingly insufficient.

A military airport is a surface facility covering approximately 600–700 hectares with a perimeter of 20–30 kilometers (Kołata 2019, pp. 37–38). It is located on land owned by the state treasury and managed by organizational units subordinate to the Ministry of National Defense. Registered in the official list of military airports and landing sites, it comprises numerous facilities and linear structures that are difficult

to conceal from adversaries equipped with modern reconnaissance technologies (Depczyński et al. 2022, pp. 74–76).

The infrastructure of a military airport includes technical zones for aircraft servicing, air traffic control and safety facilities, aircraft dispersal areas, command and logistical structures, technical and warehouse facilities, administrative offices, and barracks (Zajkowski 2020, pp. 78–80). Additionally, various logistics elements are deployed within the airport to support combat readiness and operational tasks for different types of aircraft. The type, scale, and composition of such infrastructure depend on how the airfield is intended to be used in combat operations. Military airports can be either natural or artificial, and are classified based on the type of aircraft, operational profile, runway characteristics, and mission requirements (Zajkowski 2020, pp. 81–83).

Security planning must account for a wide spectrum of threats. External threats may stem from organized crime groups, terrorist cells, opportunistic individuals exploiting weak protection, or foreign intelligence operatives (Price and Forrest 2024, pp. 45–48). Even local residents or adolescents seeking to breach restricted areas or steal military equipment pose potential risks. Moreover, regular enemy forces, including land, air, naval, or special operations units, may target airports during pre-conflict or wartime periods (Price and Forrest 2024, pp. 49–52).

Internal threats originate from within the unit, including personnel with access to sensitive areas. These may involve warehouse workers attempting to conceal losses, individuals with maintenance or cleaning duties in technical zones, or guards and staff with privileged access. Security risks are exacerbated by the fact that military airports are often situated in forested areas, enabling easier intrusion and surveillance (Price and Forrest 2024, pp. 53–55).

Several physical characteristics make military airports vulnerable to detection and attack despite camouflage efforts. These include the distinctive layout of runways and taxiways, the dispersal areas saturated with aviation equipment, electromagnetic emissions from active devices, heavy air traffic with acoustic signatures from engines, and consistent vehicle movements within the premises (Lykou et al. 2020, pp. 3–6). These features can be exploited by adversaries to identify, locate, and target critical infrastructure.

The expansive layout of a military airport provides some resilience by dispersing high-value assets, thereby mitigating the impact of attacks. However, this same dispersal complicates efforts to secure the facility as a whole. Airports are attractive targets due to their size, the dispersion of critical components, the high number of personnel involved in daily operations, and the accumulation of flammable or sensitive materials (Lykou et al. 2020, pp. 5–7; Menzel and Hesterman 2018, pp. 119–122; Usmany et al. 2025, pp. 21–26). Furthermore, the complexity of aviation systems and the relative ease of disrupting airport operations make them vulnerable to both sabotage and unconventional threats.

To mitigate these vulnerabilities, military airports are surrounded by extensive fencing (typically up to 17 km in length), illuminated, and protected by intrusion alarm systems. Guard posts, pass offices, and surveillance centers provide further control (Menzel and Hesterman 2018, pp. 123–125). Nonetheless, certain airport components remain impossible to fully conceal or shield from detection by advanced enemy systems.

Threats to military airports are diverse and include non-military risks such as weather conditions or technical failures, as well as military and terrorist threats. Military threats may involve ground assaults or air strikes carried out by manned aircraft, missiles, unmanned aerial vehicles, or civilian aircraft used for hostile purposes (Menzel and Hesterman 2018, pp. 126–128; Farahani et al. 2018, pp. 138–140). Terrorist attacks may be airborne, ground-based, or directed from outside the facility (Farahani et al. 2018, pp. 140–142; Mani and Goniewicz 2024, pp. 3–5). Among the many facilities that comprise an airbase, some have particular operational importance for Air Force missions and must therefore be prioritized for defense and protection.

This study conceptualises and analyses a multilayered security architecture for military airbases under contemporary hybrid threat conditions, integrating legal, organizational, technical and planning dimensions within a systems-based perspective. The focus is on identifying critical infrastructure vulnerabilities, evaluating protective mechanisms, and proposing a holistic framework for airbase protection in the age of hybrid warfare. The study is based on doctrinal sources, normative frameworks, and practical solutions currently in use in NATO and Polish military infrastructure.

Literature verification

Research on the security of military airbases is situated at the intersection of several academic domains, including security studies, military science, critical infrastructure protection, aviation security, and strategic studies. In both international and Polish literature, military airbases are consistently conceptualized as critical strategic assets whose disruption may significantly impair air power projection, operational readiness, and deterrence capabilities (Kołata 2019, pp. 37–39; Grenda 2023, pp. 21–24). This perspective reflects a broader understanding of airbases not merely as technical facilities, but as complex socio-technical systems embedded within national and allied defence architectures.

A substantial body of international literature focuses on physical and technical protection measures applied to airports, with particular emphasis on perimeter security, fencing systems, access control mechanisms, surveillance technologies, and rapid response arrangements. Traditional, perimeter-centric protection models,

largely inherited from Cold War-era security thinking, are increasingly assessed as insufficient in contemporary threat environments (Price and Forrest 2024, pp. 41–44; Menzel and Hesterman 2018, pp. 118–120). These studies highlight the growing mismatch between static protection concepts and dynamic, adaptive threat actors, particularly non-state and hybrid adversaries.

Within this stream of research, airports, both civilian and military, are frequently analysed through the lens of layered or defence-in-depth architectures, combining physical barriers with electronic detection systems and human patrols. While these contributions provide valuable technical insights, they tend to treat individual security components in relative isolation, often privileging technological solutions over organizational, legal, or procedural dimensions. As a result, they offer limited guidance on how different elements of the protection system interact in practice, especially under conditions of complex, multi-vector threats.

In recent years, particular attention has been devoted to emerging threats associated with unmanned aerial systems (UAS) and cyber operations. A growing number of studies demonstrate that low-cost UAVs, commercially available sensors, and cyber tools can effectively bypass conventional security arrangements, exposing structural vulnerabilities in both civilian and military aviation infrastructure (Lykou et al. 2020, pp. 4–7; Konert and Kasprzyk 2020, pp. 484–487; Goniewicz and Khorram-Manesh 2026, pp. 63–66; Goniewicz 2025, pp. 26–37). These analyses emphasize that the accessibility and affordability of such technologies significantly lower the entry threshold for hostile actors, thereby increasing the frequency and diversity of potential attack scenarios.

The literature on counter-UAS measures and cyber defence has expanded rapidly, particularly in the context of NATO and EU security debates. However, much of this research remains technocentric, focusing on detection sensors, jamming systems, or cyber countermeasures without sufficient consideration of organizational readiness, legal mandates, command-and-control arrangements, or personnel training. Consequently, while the technological dimension of airbase protection is well represented, its integration into broader security governance frameworks is often underdeveloped.

Another important analytical strand concerns hybrid threats, understood as the coordinated use of military and non-military instruments such as sabotage, cyberattacks, disinformation, economic pressure, and irregular tactics. Within this framework, military airbases are identified as particularly attractive targets due to their spatial dispersion, organizational complexity, and concentration of critical assets (Farahani et al. 2018, pp. 137–140; Mani and Goniewicz 2024, pp. 4–6). Hybrid threat literature stresses that attacks on airbases may occur below the threshold of armed conflict, blurring the distinction between peacetime and wartime security regimes.

In Polish literature, the issue of military airport security is addressed primarily within the fields of military science and critical infrastructure protection. Existing

studies provide detailed descriptions of organizational structures, legal frameworks, and protection systems applied within the Polish Armed Forces, forming an important empirical and normative foundation, particularly with regard to national regulations, internal instructions, and operational doctrines (Kołata 2019, pp. 38–41; Grenda 2023, pp. 17–22; Bogusz 2024, pp. 55–59). At the same time, this body of work often adopts a predominantly descriptive or instructional perspective, focusing on the organization of protection systems rather than offering a critical assessment of their adequacy in relation to evolving threat environments.

A recurring limitation in both international and national literature is the fragmentation of analytical perspectives. Legal regulations, organizational arrangements, technical measures, and planning processes are frequently examined as separate domains, with limited effort to integrate them into a coherent analytical framework. Studies that explicitly address planning and risk management processes in military airbase security remain relatively scarce, despite the central role of planning in shaping the effectiveness and adaptability of protection systems.

Moreover, while several authors acknowledge the importance of human factors, such as personnel training, decision-making, and inter-agency coordination, these aspects are rarely operationalized within comprehensive analytical models. This gap is particularly visible in the context of cooperation between military units, law enforcement agencies, and private security providers, which is increasingly relevant for airbase protection in hybrid threat scenarios.

In summary, the existing body of literature provides substantial insights into individual components of military airbase security, particularly in the technical and physical domains. However, comprehensive analyses that integrate legal, organizational, technical, and planning dimensions within a single, system-based perspective remain limited. The present study responds to this gap by synthesizing doctrinal, regulatory, and academic sources into a holistic analytical framework, thereby contributing to both national and international debates on the protection of critical military infrastructure in an evolving hybrid threat environment.

Research methodology

This study employs a qualitative, non-empirical research design based on a structured narrative review and conceptual analysis of sources related to the security of military airbases. The adopted methodology is appropriate given the exploratory and system-oriented character of the research problem, as well as the limited accessibility of empirical data due to the classified nature of many operational aspects of military infrastructure protection.

The research process was conducted in several sequential stages. In the first stage, the scope of analysis was defined by identifying key thematic areas relevant to military airbase security under hybrid threat conditions. These areas included: legal and organizational frameworks, physical protection systems, technical security measures, zonal defense architecture, and planning and risk management processes. This thematic structure guided both the selection of sources and the subsequent analytical procedure.

The study adopts a systems-based and defence-in-depth analytical perspective, treating airbase security as an integrated and multilayered protection architecture rather than a collection of isolated technical solutions.

In the second stage, source identification and selection were carried out. The analyzed materials comprised NATO doctrinal documents, national regulations and instructions of the Polish Armed Forces, publicly available military guidelines, technical standards, and peer-reviewed academic publications. Sources were selected purposively rather than exhaustively, with priority given to documents directly addressing military or critical infrastructure protection, aviation security, hybrid threats, and risk management. Only declassified and open-source materials published between 2000 and 2023 were included in the analysis.

The third stage involved qualitative content analysis of the selected materials. Each source was examined with regard to its contribution to understanding threat typologies, protection mechanisms, organizational arrangements, and planning principles applicable to military airbases. The analysis focused on identifying recurring concepts, normative assumptions, and recommended practices, as well as inconsistencies and gaps between doctrinal prescriptions and emerging threat characteristics. Particular attention was paid to how individual security components are conceptualized and whether they are treated in isolation or as part of an integrated protection system.

In the fourth stage, the findings from different source categories were compared and synthesized across the predefined thematic domains. This cross-domain analysis enabled the identification of systemic vulnerabilities and interdependencies between legal, organizational, technical, and human factors. Rather than evaluating the effectiveness of individual technologies or procedures in isolation, the study emphasizes their functional integration within a coherent security architecture.

The final stage consisted of conceptual synthesis, leading to the development of a holistic and practice-oriented framework for military airbase protection. This framework reflects the combined insights derived from doctrinal analysis, regulatory review, and academic literature, and is intended to support security planning and decision-making at the organisational level rather than operational-level implementation.

Due to the absence of primary empirical data, the study does not employ statistical analysis or field-based validation. Instead, methodological rigor is ensured

through transparent source selection, explicit analytical criteria, and systematic structuring of the review process. This approach allows for analytical generalization and theoretical insight while remaining consistent with the constraints inherent to research on sensitive military infrastructure, as well as the refinement and implementation of protective measures at military airbases.

Review of protective measures

Proper protection of combat equipment and weapons, ammunition and explosives, as the most important military property, requires efficient physical protection and comprehensive technical safeguards forming an integrated security system (Lavrentyev et al. 2019, pp. 2–4). Airport security encompasses a set of activities aimed at preventing hidden and unauthorized access to protected premises, where the intent may involve the destruction or neutralization of military equipment and technology. The purpose of such protection is to ensure order and safety within the facility and to counteract acts of diversion or manifestations of terrorism (Lavrentyev et al. 2019, pp. 5–7; Nowak et al. 2020, pp. 76–78).

Protective measures are intended to provide effective direct and indirect protection of specific facilities and personnel that may be subject to reconnaissance or attacks by conventional and subversive enemy forces, as well as terrorist or criminal groups (Michalski and Radomyski 2019, pp. 54–57). In order to ensure the safety of the facility, it is necessary to construct an appropriate protection system, which requires comprehensive reconnaissance of the object and precise identification of the nature of potential threats (Kustra and Nowakowski 2020, pp. 286–289).

Concept of Facility Security Systems

To ensure the proper effectiveness of protective activities, it is advisable to establish a security system within the facility consisting of a number of interrelated elements. This system is designed to ensure the safety of people and property, as well as the undisturbed functioning of the facility. The creation of a facility security system is preceded by preliminary activities aimed at comprehensive reconnaissance of the site and precise determination of the nature and scope of security services (Skorupski and Uchroński 2018, pp. 54–56). At this stage, the concept of a facility security system may be defined as the coordinated application of specific forces and means within the facility to ensure the protection of people and property in accordance with identified threats and the prevailing legal framework (Skorupski and Uchroński 2018, pp. 56–58).

It can be assumed that the core elements of a facility's security system include legal and organizational measures, technical solutions, and protective or intervention forces. These three dimensions—organizational structures, technical safeguards,

and human action—together constitute the comprehensive security architecture of a military facility (Dandeker 2021, pp. 176–179). A complementary conceptualization defines the protection system as comprising all organizational and technical factors, together with their mutual relations and interactions with the operational environment, designed to effectively counteract potential threats. This perspective supports the view that a properly structured protection system enables optimal utilization of its components, particularly when these elements function in a coordinated and mutually reinforcing manner (Wójcik 2003, pp. 112–115).

Legal and organizational measures refer broadly to the applicable legal frameworks that shape the design, implementation, and operation of the security system. These include general legislative acts as well as specific internal regulations adapted to the operational context of a particular facility. Legal regulations may govern a wide range of domains, such as construction standards, fire protection, energy efficiency, and sanitary requirements (Bogusz 2024, pp. 61–64). They also specify rules for the storage of weapons, as well as the use and transport of hazardous substances—including toxic, radioactive, explosive, or flammable materials—and the handling of dangerous installations such as electrical systems, gas networks, weapons, and ammunition (Konert and Kasprzyk 2020, pp. 486–489).

In addition, legal and organizational instruments regulate the internal safety management of the facility. This includes institutional documents such as security plans, operational instructions, procedures, and clearly defined areas of responsibility. They outline the competencies, tasks, and accountability of designated personnel and departments in the realm of security. Finally, they also define the structure and mandate of both physical and technical protection forces, as well as the supervisory bodies that support and monitor security-related operations.

Technical measures constitute a fundamental element of a facility's security system and encompass all devices and systems of a technical nature used to prevent or respond to threats. These measures can be broadly divided into three categories: constructional, mechanical, and electronic.

Constructional measures refer to the physical elements of a building or infrastructure that inherently provide structural protection. These include walls, ceilings, floors, roofs, entrances and exits, staircases, passageways, architectural layouts, adjacent constructions, windows and doors of standard design, as well as various types of perimeter fencing. Their configuration and structural resilience are crucial in delaying or preventing unauthorized access and in shaping the defensive architecture of the airbase (Rurak and Goniewicz 2024, pp. 6–8).

Mechanical means are defined as reinforcements or protective solutions applied to building components and designated spaces, often in conjunction with electronic systems. This broad category includes window protection such as reinforced glass, shutters, metal grates, roller shutters, and security films. Door and entrance

reinforcements may consist of specialized security doors, locks, padlocks, bars, and automated roller systems (Bogusz 2024, pp. 66–69; Konert and Kasprzyk 2020, pp. 487–490; Rurak and Goniewicz 2024, pp. 8–10). Additionally, mechanical security encompasses fixed devices for securing assets, such as steel and armored cabinets, safes, and locked containers, as well as portable solutions including handheld security cassettes, steel cases, and protective briefcases. Dedicated rooms for storing valuable materials also fall within this category.

Electronic security systems complement and extend the reach of physical and mechanical protection. These systems include intrusion detection systems (burglary and sabotage alarms), access control mechanisms, fire detection and suppression systems, and closed-circuit television (CCTV) used for surveillance and real-time monitoring (Bogusz 2024, pp. 69–72; Konert and Kasprzyk 2020, pp. 490–493; Rurak and Goniewicz 2024, pp. 10–12). Their integration with physical infrastructure enables layered protection and enhances the overall effectiveness of the security system by supporting early detection, situational awareness, and rapid response.

In the context of military airport security, technical measures operate alongside two other key components: operational procedures and physical protection. The interaction of these three domains forms a comprehensive protection strategy. Procedures, derived from formal regulations, orders, and internal policies, govern the actions and responsibilities of security personnel and military officers (Radomyski and Bernat 2018, pp. 261–264). These include general command procedures related to planning, organizing, supervising, and controlling operations, as well as highly specific instructions formalized in Permanent Operating Procedures (POP) (Ryczyński et al. 2025, pp. 4–6). Together, these procedures determine standardized patterns of conduct for personnel involved in airbase security operations and constitute the procedural backbone supporting technical and physical protection systems.

Physical protection at a military airport is based on an organized system involving duty services and civilian guard units or specialized armed protective formations operated by licensed private security companies. Within this structure, the duty officer plays a central role, acting as the direct executor of the commander's decisions (Nowak et al. 2020, pp. 76–78). This officer supervises the activities of subordinate services, including duty subunits, fire response units, and technical equipment facilities, and is responsible for the overall security of military installations and equipment (Nowak et al. 2020, pp. 78–80; Dandeker 2021, pp. 178–181; Wójcik 2003, pp. 114–117; Bogusz 2024, pp. 72–75).

In parallel, airports may be protected by Specialized Armed Protection Formations or Civil Guard Units. Specialized Armed Protection Formations are private entities established by individuals licensed to conduct personal and property protection services and authorized to carry firearms. These entities are selected through public procurement procedures and operate under contracts governed by defence regulations, including the Regulation of the Minister of National Defense and the

Instruction on the Protection of Military Facilities (OIN 3/2008) (Piekarski 2022, pp. 3–6). Personnel employed in these formations must meet specific requirements, including clearance for classified information, depending on the expectations of the military unit. Their core responsibilities involve the protection of military infrastructure as well as the escorting of personnel, cargo, and equipment. Guards are licensed at two professional levels and are authorized to cooperate with state services such as the Police, fire services, civil defence units, and municipal guards (Dandeker 2021, pp. 179–182; Wójcik 2003, pp. 116–119; Bogusz 2024, pp. 75–78).

Employees of Specialized Armed Protection Formations are legally entitled to conduct identity checks, perform personal searches, detain individuals, and apply direct coercive measures. These may include batons, handcuffs, stun guns, incapacitating gas, or firearms. The scope of these powers is strictly regulated under the Act on the Protection of Persons and Property, in particular Articles 36–38, which define the permissible range of actions both within and outside protected zones (Dandeker 2021, pp. 180–183; Wójcik 2003, pp. 118–121; Bogusz 2024, pp. 78–81; Konert and Kasprzyk 2020, pp. 488–491).

Civil Guard Units, on the other hand, are established upon the request of the military unit's commander and approved by the relevant command structures of the Polish Armed Forces. These units play a complementary role in enforcing airport security.

Technical protective measures at military airports are designed to ensure the safety of both aircraft and personnel. Central to this objective is the establishment of access control systems and the regulation of movement within secured airport zones. A network of properly organized control posts and mobile patrols enhances the facility's capability to detect, deter, and respond to unauthorized access or emerging threats (Dandeker 2021, pp. 181–184; Wójcik 2003, pp. 120–123; Bogusz 2024, pp. 81–84; Konert and Kasprzyk 2020, pp. 489–492).

The protection of military airports encompasses several interrelated domains, including the safeguarding of infrastructure, personnel, and documentation; ensuring information and communication technology (ICT) security; restoring operational capacity following disruption; neutralizing explosive threats; providing health protection; enforcing fire safety; and repairing damage resulting from enemy attacks (Radomyski and Bernat 2018, pp. 262–266; Ryczyński et al. 2025, pp. 5–7; Piekarski and Wojtasik 2022, pp. 4–6). Each of these areas requires targeted planning measures and dedicated resources adapted to the specific operational context of the facility.

Because of the diverse nature of military airport infrastructure, including its varying sizes, layouts, and functions, protection strategies must be customized rather than generalized. This demands the application of security measures tailored to the characteristics of each site and grounded in a logic of proportionality and interdependence.

Protection may take the form of a permanent or temporary physical presence, supported by direct monitoring of signals from electronic alarm systems. Technical maintenance services are essential for the correct installation, operation, and repair of both electronic devices and mechanical protective systems (Dandeker 2021, pp. 182–185; Wójcik 2003, pp. 121–124; Bogusz 2024, pp. 84–87; Konert and Kasprzyk 2020, pp. 490–493). These services include the installation and maintenance of alarm systems, motion detectors, locking mechanisms, and emergency access points.

Forms of direct physical protection range from fixed guard posts operating on a 24/7 basis to relief posts activated in response to situational needs. Additional measures include patrols along designated routes, mixed patrol and round systems, and mobile intervention groups responsible for verifying alarm signals and taking appropriate action (Dandeker 2021, pp. 185–188; Wójcik 2003, pp. 124–127; Bogusz 2024, pp. 87–90; Konert and Kasprzyk 2020, pp. 493–496; Piekarski and Wojtasik 2022, pp. 6–8). Supervision of alarm signals transmitted via visual, acoustic, or digital channels is typically integrated with intervention response systems, enabling real-time threat verification and rapid deployment of protective measures.

The above-mentioned elements form the foundation of a professional airport security system, which is organized into four primary protective zones: peripheral protection, perimeter external protection, direct external protection, and internal protection. The physical protection of facilities is ensured through a combination of fencing systems, concrete barriers constructed from prefabricated elements, steel--profile gates at both main and auxiliary entry points, technical solutions, internal security services, and an integrated access control system (Dandeker 2021, pp. 186–189; Wójcik 2003, pp. 127–130; Piekarski and Wojtasik 2022, pp. 8–10; Kierzkowski et al. 2024, pp. 3–5). Access control is implemented through both technical measures, such as electronic access card readers, and physical means involving personnel responsible for verifying individual authorizations.

To enhance safety across the military airport, designated pedestrian and vehicle traffic zones are established. These areas are subject to continuous supervision and may be restricted when operationally required. The peripheral protection zone encompasses the area located beyond the external fence of the military facility. Although alarm systems are not installed within this zone, a strip approximately 25 meters wide is maintained free of high vegetation, including bushes and tall grasses (Kierzkowski et al. 2024, pp. 5–7; Mieloszyk et al. 2018, pp. 50–52). This cleared space enables unobstructed observation and access to the surroundings of the protected facility. However, this zone is not maintained when it extends beyond land administered by military authorities.

The perimeter external protection zone lies between the outer and inner fencing of the military site. Within this zone, various protective devices and alarm systems are installed, including lighting, wired communication systems for security forces, and surveillance infrastructure. This area should include at least two independently

functioning alarm systems, for example a combination of fencing and surface systems, fencing and underground systems, or dual surface systems such as active infrared beams and microwave barriers. Under adverse weather conditions, the effective detection range must not fall below 60% of the nominal range for infrared systems and 80% for microwave systems (Mieloszyk et al. 2018, pp. 52–55). These performance thresholds do not apply to video detection technologies.

The direct external protection zone refers to areas of land immediately surrounding key structures, such as warehouses or operational buildings located within the facility. In this zone, external alarm systems configured to cooperate with closed-circuit television (CCTV) cameras are deployed. These systems may include ground-based, underground, or fencing-mounted sensors, selected according to the dimensions, function, and specific security requirements of each building. Alarm systems operating within this zone are primarily responsible for initiating surveillance verification and must be fully integrated with the facility's broader monitoring and response infrastructure (Radomyski and Bernat 2018, pp. 264–266).

The internal protection zone encompasses the interior spaces of warehouses and buildings, including windows, doors, ventilation openings, and other potential access points. This zone is equipped with internal alarm systems that may operate in conjunction with CCTV systems and other protective devices. In high-security areas, such as armament storage facilities, internal alarm systems must include at least two different types of detectors operating on distinct principles, for instance, combining infrared with microwave or ultrasonic detectors. If small arms are stored in areas with regular glass windows, glass-break detectors must also be installed. Crucially, the layout of the alarm system must eliminate so-called "blind spots" where intruders might remain undetected. The use of dual-technology detectors in weapons storage or other highly secured rooms is explicitly discouraged to prevent potential system vulnerabilities.

Personnel protection is implemented by individually equipping soldiers with specialized weapons and equipment, including anti-fragmentation vests, protective clothing, and individual medical kits. These measures are accompanied by the development of appropriate operating and conduct procedures. Depending on the assessed threat level, specific codes for clothing and personal equipment may be introduced, such as firearms, bulletproof vests, helmets, or protective gear against contamination. To minimize the risk of surveillance or attacks by hostile forces or intelligence services, the dissemination of sensitive information is tightly controlled (Kierzkowski et al. 2024, pp. 6–9). This includes restricting knowledge of convoy movements, the presence of task forces, visits by command or coalition personnel, as well as the timing and location of briefings, meetings, and key staff gatherings.

The responsibilities of the Personnel Protection Team include access control at all entry points, which are equipped with metal detectors and thermal imaging cameras. In addition, engineering measures may be implemented to prevent

unauthorized vehicle entry, particularly vehicles carrying improvised explosive devices. Specialized protection teams provide direct physical security for personnel using body armor and armored transport vehicles (Mieloszyk et al. 2018, pp. 53–56; Nowacki and Paszukow 2018, pp. 188–191). In the event of chemical or biological threats, soldiers are equipped with appropriate contamination protection. Access to official premises is restricted according to assigned roles and clearance levels in order to limit information exposure. Counterintelligence monitoring is also applied to external personnel operating at the airport, such as contractors or Host Nation Support (HNS) staff.

The core elements of the personnel protection system include Entry Control Points (ECPs), Command Post Protection (DOC), and Key Personnel Protection (KP). The physical security of command posts, the Tactical Area of Responsibility (TAOR), and senior officers is ensured through dedicated security teams. These units may be tasked with access control duties or the direct protection of commanders (Karpiuk and Kelemen 2022, pp. 72–75). Responsibility for troop protection is also vested in commanders at successive levels of command.

To secure classified information, documents are stored in designated areas such as public and classified registries or foreign document service points. Within workstations, information is kept in safes or armored containers in accordance with national or coalition standards. Security procedures define access protocols, and any unauthorized attempt to breach secured zones triggers formal response procedures (Mieloszyk et al. 2018, pp. 55–58). Printed documents containing personal data, including names, ranks, and addresses, must be destroyed after use. Planning materials, handwritten notes, and maps are either returned to authorized repositories or disposed of in accordance with classification guidelines (Karpiuk and Kelemen 2022, pp. 75–78).

To prevent unauthorized access to confidential or higher-level information, a multilayered structure is implemented. This includes the establishment of protection zones, monitoring of zone entry and exit, individualized authorizations, and certified devices for information protection. Access to the airport area is controlled through designated entry points (ECP, EECP, EG) with permanent passes used to regulate movement within specific zones.

Three levels of security zones are defined. Zone I permits direct access to top-secret or secret materials and requires the highest physical security standards, including Class I burglary-resistant rooms. Zone II restricts direct access to classified data and requires the storage of materials in certified metal containers. Zone III functions as a general access control zone with no exposure to sensitive information (Karpiuk and Kelemen 2022, pp. 78–81).

Information and communication technology (ICT) security is ensured by appointing designated officers responsible for safeguarding classified information within digital systems. Personnel granted access must hold NATO-level security

clearance corresponding to the classification level of the information processed. Special procedures governing the secure operation of ICT systems are implemented to ensure compliance and mitigate operational risks (Tynan et al. 2019, pp. 6–9). Non-authorized individuals requiring access to secure areas must remain under continuous supervision to prevent the disclosure of information via computer screens or printed materials. Furthermore, private mobile phones and recording devices are prohibited within secure zones, and all classified communications must be conducted exclusively through protected channels or within designated secure areas.

Planning of security measures for a military airport

Planning is a universal activity practiced by all organizations, though no two organizations plan in the same way. In modern settings, planning is a time-consuming and complex process that must consider many internal and external factors. Effective planning requires an understanding of one's own strengths and weaknesses, as well as the financial, material, and human resources available. Through detailed analysis, planners can identify the optimal course of action and develop a sound action plan.

In the literature, planning is understood in multiple ways. It is defined as the analysis of internal and external conditions of action and the design of appropriate means and methods of action, adjusted both to objectives and operational conditions (Zimmermann and Duffy 2023, pp. 313–315). Another definition describes planning as a preparatory and design-oriented activity aimed at constructing a set of objectives and the operational structure for their implementation (Malakis et al. 2023, pp. 4–6). In a broader sense, planning involves identifying optimal future solutions for achieving defined goals.

Effective planning of protective measures for a military airport begins with acquiring comprehensive knowledge of the facility, the conditions under which it operates, the spectrum of potential threats, and the resources available to mitigate those threats. This process involves cognitive, analytical, and investigative activities aimed at identifying existing or potential risks to personnel, infrastructure, and operational assets (Malakis et al. 2023, pp. 6–8).

Several methods support this reconnaissance process. Local vision involves direct contact with the protected site and includes assessing the nature of the facility (e.g., warehouses, fuel depots, airport control towers), its location within the airport premises, surrounding terrain and adjacent structures, accessibility, internal layout, as well as distances from perimeter boundaries and patrol response times (Stolzer et al. 2023, pp. 96–99).

Documentation such as architectural designs, technical schematics of alarm systems, and organizational diagrams provides additional insight into the facility's structure and operational context (Chan and Li 2023, pp. 3–5; Natalia et al. 2025,

pp. 7–9). Further sources of information include crime statistics in the vicinity of the facility, reports on previous security incidents, and coordination with external security services such as the Military Police and local police units. It is also essential to assess organizational determinants of daily operations, including personnel rotation patterns, material flows, and operational schedules.

Only when the object of protection is sufficiently known and its operating conditions clearly defined can protective measures be properly planned. Such knowledge should include its location in relation to other facilities, separation methods, specific characteristics that may pose risks, and existing security mechanisms.

Although planning is essential, normative documents of the armed forces rarely provide a standardized planning methodology. A structured seven-stage planning framework has been proposed, beginning with task analysis aimed at identifying objectives and the factors influencing the organization of security (Grenda 2023, pp. 32–35). This stage is followed by an assessment of the current situation, including the identification of existing threats and internal vulnerabilities. The next phase involves risk assessment, focusing on the probability and potential consequences of identified threats, followed by risk management activities aimed at reducing these risks to acceptable levels (Grenda 2023, pp. 36–40).

After these analyses, planners consider possible courses of action. Typically, two or three options are developed and evaluated according to uniform criteria. The optimal variant is selected to serve as the foundation for a tailored protection strategy.

The next step is the formulation of a protection system concept. This concept defines the structure, functions, technical resources, command model, and key security components. Once completed, it provides a blueprint for implementation and resource allocation. The concept is often presented as a document supplemented with diagrams or maps, detailing the aims of protection, legal constraints, vulnerabilities, types of threats, proposed countermeasures, and operational timelines.

Following approval of the concept, the actual airport security plan is developed. This plan includes a threat assessment, inventory of existing protection systems, and a description of the organizational and technical security structure, including personnel, equipment, and procedures. It becomes an annex to the base commander's order and a cornerstone document for the implementation and coordination of all security operations at the military airport.

Limitations

While this article provides a comprehensive overview of protective measures and planning processes related to military airport security, several limitations should be acknowledged.

First, the analysis is based primarily on normative frameworks, doctrinal assumptions, and selected operational concepts applicable within the Polish and NATO military context. As such, some of the recommendations may not fully translate to civilian airports or non-NATO defense environments, where organizational structures, legal standards, and threat perceptions may differ.

Second, the article does not include empirical data from real-life military airport operations, such as post-incident assessments, training simulations, or audits. This limits the ability to evaluate the practical effectiveness or operational efficiency of the described security components.

Third, while the article highlights technological and organizational measures, it does not systematically evaluate their cost-effectiveness, implementation challenges, or human factors, which are critical in real-world operations.

Finally, the evolving nature of hybrid threats, cyber warfare, and unmanned aerial systems presents dynamic challenges that require continuous adaptation, aspects only briefly addressed in the planning framework. Future studies should aim to validate and refine the proposed security planning concepts through empirical research, scenario-based assessments, or simulation-based testing.

Conclusions

This article has reviewed the core components of protective systems at military airports, emphasizing the dynamic interplay between technical measures, organizational structures, and human resources. A comprehensive and systematic approach to facility security, anchored in system integration, layered defence principles, adaptive risk management, coordinated threat analysis, and inter-agency operational coordination, is essential for safeguarding critical aviation infrastructure in the face of evolving and hybrid threats.

The multi-layered structure of protective measures, which includes physical protection, personnel security, zonal defense architecture, and ICT safeguards, illustrates the increasing complexity of contemporary security environments. Among these, planning emerges as a cornerstone of effective protection, requiring in-depth knowledge of protected assets, their vulnerabilities, and the contextual environmental factors.

Looking ahead, the development of military airport security systems should incorporate adaptive risk management strategies, integration of advanced technologies, and improved interoperability between military, law enforcement, and private security actors. These enhancements will ensure resilience and responsiveness in both peacetime and crisis scenarios.

The presented framework offers a structured reference for national defense authorities and NATO-aligned actors aiming to refine critical infrastructure protection

frameworks. Ultimately, the effective security of a military airport should be understood as the synergistic combination of capable protective forces and robust technical infrastructure, forming a coherent, multilayered and dynamically integrated security architecture.

BIBLIOGRAPHY

1. Bogusz, D., 2024. Polish Air Force. Warsaw: Publishing House prof. Leszek J. Krzyżanowski Warsaw Management University.
2. Chan, W.T. and Li, W.C., 2023. Development of Effective Human Factors Interventions for Aviation Safety Management. Frontiers in Public Health, 11, 1144921.
3. Dandeker, C., 2021. On 'the Need to Be Different': Recent Trends in Military Culture. In: The British Army, Manpower and Society into the Twenty-First Century. London: Routledge, 173–187.
4. Depczyński, M., Markiewicz, S. and Wrzosek, M., 2022. Challenges and Threats to Military Reconnaissance and Radio Combat from the Aspect of the Anti-Access System. The Journal of Slavic Military Studies, 35(1), 73–93.
5. Farahani, G.J., Kachoee, M.H. and Kachoee, M.A., 2018. Vulnerability Assessment of Critical Infrastructure against Man-Made Threats: Case Study of International Civilian Airports. Industrial Engineering & Management Systems, 17(1), 136–145.
6. Goniewicz, K. and Khorram-Manesh, A., 2026. Resilience and Recovery in Disaster and Emergency Management. London: Academic Press.
7. Goniewicz, K., 2025. Autonomous and Artificial Intelligence-Enabled Drone Systems for Medical Triage: A State-of-the-Art Review of Emerging Technologies and Swarm Applications. Emergency Health Services Journal, 2(2), 26–37.
8. Grenda, B., 2023. Bezpieczeństwo Lotnisk Wojskowych. Warsaw: Wydawnictwo ASzWoj.
9. Karpiuk, M. and Kelemen, M., 2022. Cybersecurity in Civil Aviation in Poland and Slovakia. Cybersecurity and Law, 8(2), 70–83.
10. Kierzkowski, A., Ryczyński, J., Kisiel, T. and Mardeusz, E., 2024. Influence of the Configuration of Airport Security Control Systems on the Implementation of Assumptions of the Sustainable Development Policy. Sustainability, 16(20), 8750.
11. Kołata, G., 2019. Airbase as Defended Asset for Air Defense. Safety & Defense, 5(1), 37–45.
12. Konert, A. and Kasprzyk, P., 2020. Drones Flying Outside Segregated Airspace in Poland: New Rules for BVLOS UAV Operations. Journal of Intelligent & Robotic Systems, 100(2), 483–491.
13. Kustra, M. and Nowakowski, H., 2020. Counteracting Unmanned Aerial Systems in the Operational Area of Airports. Journal of KONBiN, 50(2), 285–293.
14. Lavrentyev, O., Gorshkov, V., Zubkov, B., Pleshakov, A., Popov, Y. and Guziy, A., 2019. Protection of Civil Aviation Aircraft Involved in the Carriage of Dangerous Goods against Acts of Unlawful Interference and Emergency Situation Prevention. International Journal of Civil Engineering and Technology, 10(3), 1–10.

15. Lykou, G., Moustakas, D. and Gritzalis, D., 2020. Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies. Sensors, 20(12), 3537.
16. Malakis, S., Kontogiannis, T. and Smoker, A., 2023. A Pragmatic Approach to the Limitations of Safety Management Systems in Aviation. Safety Science, 166, 106215.
17. Mani, Z. and Goniewicz, K., 2024. Assessing the Public Health Implications of Aviation Terrorism: A Retrospective Analysis of Global Trends and Response Strategies. Disaster Medicine and Public Health Preparedness, 18, e272.
18. Menzel, D. and Hesterman, J., 2018. Airport Security Threats and Strategic Options for Mitigation. Journal of Airport Management, 12(2), 118–131.
19. Michalski, D. and Radomyski, A., 2019. Modern Aspects of the Development of Security in Air Transport under the Conditions of Air Terrorism. Security and Defence Quarterly, 26(4), 51–66.
20. Mieloszyk, E., Milewska, A. and Wyroślak, M., 2018. Increasing the Country's Security and Public Transport Accessibility by Creating a Network of Small Airports. Zeszyty Naukowe Akademii Sztuki Wojennej, 113(4), 49–60.
21. Natalia, Y.A., De Cauwer, H., Neyens, T., Goniewicz, K., Somville, F. and Molenberghs, G., 2025. A Bayesian Network Analysis of Aviation Terrorism Attack Risks. Journal of Transportation Security, 18(1), 1–17.
22. Nowacki, G. and Paszukow, B., 2018. Security Requirements for New Threats at International Airports. TransNav: International Journal on Marine Navigation and Safety of Sea Transportation, 12(1), 187–192.
23. Nowak, J., Achimowicz, J., Ogonowski, K. and Biernacki, R., 2020. Protection of Air Transport against Acts of Unlawful Interference: What's Next? Safety & Defense, 2, 75–88.
24. Piekarski, M. and Wojtasik, K., 2022. Protection of Polish Critical Infrastructure against Air Threats. Security and Defence Quarterly, 39, 1–12.
25. Price, J. and Forrest, J., 2024. Practical Aviation Security: Predicting and Preventing Future Threats. London: Elsevier.
26. Radomyski, A. and Bernat, P., 2018. Contemporary Determinants of Organising Effective Protection of Civil Aviation against Terrorism. Transportation Research Procedia, 35, 259–270.
27. Rurak, A. and Goniewicz, K., 2024. Enhancing Security Measures for Military Air Bases: Integrating Advanced Technologies and Operational Strategies. Studia Bezpieczeństwa Narodowego, 14, 1–15.
28. Ryczyński, J., Kierzkowski, A., Nowakowska, M. and Uchroński, P., 2025. Cultural Diversity and the Operational Performance of Airport Security Checkpoints: An Analysis of Energy Consumption and Passenger Flow. Energies, 18(14), 3853.
29. Skorupski, J. and Uchroński, P., 2018. Evaluation of the Effectiveness of an Airport Passenger and Baggage Security Screening System. Journal of Air Transport Management, 66, 53–64.
30. Stolzer, A.J., Sumwalt, R.L. and Goglia, J.J., 2023. Safety Management Systems in Aviation. Boca Raton, FL: CRC Press.

31. Tynan, M.P., Prabhakar, G. and Nisar, T.M., 2019. A Qualitative Review of the Contribution of Military Leadership to Humanitarian Supply Chain Operations. In: Proceedings of the 3rd IEOM European International Conference on Industrial Engineering and Operations Management. Pilsen, Czech Republic, 1–10.
32. Usmany, J., et al., 2025. Attacks on healthcare in conflict-affected countries: a comparison of temporal trends in ongoing conflicts in Lebanon, Myanmar, occupied Palestinian territory, Sudan and Ukraine using WHO SSA and SHCC data, 2018–2024. Population Health Metrics, 21-26.
33. Wójcik, A., ed., 2003. Ocena Bezpieczeństwa Obiektów. In: Mechaniczne i Elektroniczne Systemy Zabezpieczeń, Vol. II, Part 2.12.3.1. Warsaw: Verlag Dashöfer.
34. Zajkowski, R., 2020. The Principles and Organization of Air Traffic in Military Operations: Experiences from the Mission in Iraq. Safety & Defense, 6(1), 77–88.
35. Zimmermann, N. and Duffy, V.G., 2023. Systematic Literature Review of Safety Management Systems in Aviation Maintenance Operations. Human–Automation Interaction, 311–328.