Terrorism – Studies, Analyses, Prevention, 2025, special edition: 159–183

https://doi.org/10.4467/27204383TER.25.018.21521

Article

Legal and technical methods of protecting critical infrastructure facilities against threats from unmanned aerial vehicles – the Polish example

JĘDRZEJ ŁUKASIEWICZ
https://orcid.org/0000-0002-7082-8511
Independent author

DAMIAN SZLACHTER
https://orcid.org/0000-0003-2763-9325
Internal Security Agency

Abstract

The aim of this article is to discuss the legal changes introduced in Poland in response to the growing threat to critical infrastructure facilities from unmanned aerial vehicles (UAVs) and to present a recommended method for assessing the effectiveness of UAV detection and neutralisation systems developed by the Government Centre for Security (RCB). The authors discuss the amendment of the *Act of 3 July 2002 – Aviation Law*, which includes provisions relevant to the safety of unmanned platform flights, ensuring that operators of critical infrastructure have the right to defend the protected facility against attacks using unmanned aircraft, and the amendment of the *Act of 24 May 2013 on direct coercive measures and firearms*, which expanded the catalogue of direct coercive measures to include the destruction or immobilisation of UAV or the seizure of control over its flight, and indicated the means of its neutralisation.

Keywords

critical infrastructure, unmanned aerial vehicles, Aviation Law, drone detection and neutralisation systems

Introduction

The miniaturisation of electronics, the construction of efficient energy sources used in UAVs and the relatively simple process of pilot training have all contributed to the development and popularisation of unmanned aviation. The availability of various models of these aircraft, as well as parts and manuals that allow for the independent and anonymous construction of an unmanned platform, as well as access to 3D printing technology, which allows even complex components to be made, have led to the large-scale use of UAVs in, among other things, sabotage operations, including in attacks on critical infrastructure (CI) facilities. Efforts to introduce legal and organisational solutions in Poland to provide CI operators with a chance to build effective anti-drone systems have been underway for several years[1]. The finalisation of these activities is the entry into force of the amendment to the Aviation Law (February 2025), which introduces major changes to the use of anti-drone systems by CI operators. The purpose of this article is to discuss these changes and to present the recommendations of Government Centre for Security (RCB) for a method of assessing the effectiveness of detection systems and the neutralisation of unmanned platforms.

Unmanned aerial vehicles as a tool for attacking a critical infrastructure facility

Unmanned aerial vehicles are increasingly being used as a tool for reconnaissance of CI systems or facilities and for attacks on them. In survey

[1] The authors of the article participated in the work of several inter-ministerial working groups (under the aegis of the Polish institutions: the Ministry of the Interior and Administration or the Internal Security Agency) as well as internal teams established by the Government Centre for Security or the European Commission bodies.

studies conducted among representatives of services and institutions within the counter-terrorism system in Poland, as well as government think tank analysts, UAVs were identified as the tool posing the greatest challenge for services, authorities, and institutions responsible for ensuring the security of facilities that could be targeted in a terrorist attack. Along with 3D printing, they accounted for 77.66% of all indications[2]. Until the full-scale Russian invasion of Ukraine, the use of drones in attacks on CI was rare. Warfare has contributed to the rapid development of unmanned technologies as well as to the development of new tactics for attacks using unmanned platforms.

Under current law, CI are systems and their functionally related facilities, including buildings, equipment, installations, services that are key to the security of the state and its citizens and that serve to ensure the efficient functioning of public administration bodies, as well as institutions and entrepreneurs. CI includes the following systems:

a) energy, energy raw materials and fuels supply,
b) communications,
c) ICT networks,
d) finance,
e) food supply,
f) water supply,
g) health care,
h) transport,
i) rescue services,
j) ensuring continuity of public administration,
k) production, storage, warehousing and use of chemical and radioactive substances, including pipelines for hazardous substances[3].

An unmanned aircraft system is an unmanned aircraft (a platform that floats in the air) together with the equipment for its remote control (a ground station with which the pilot can control the aircraft during flight)[4]. The legislation does not distinguish between aircraft types. The most common types of unmanned platforms include multirotors,

[2] D. Szlachter, *Terrorism in Poland and trends in its development. Survey results (summary report)*, "Terrorism – Studies, Analyses, Prevention" 2022, no. 2, pp. 335–363. https://doi.org/10.4467/27204383TER.22.029.16349.

[3] Article 3(2) of the *Act of 26 April 2007 on crisis management*.

[4] *Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft*.

aircraft, helicopters and hybrids, the design of which combines features of the other types of aircraft. A hybrid can be, for example, an aircraft equipped with additional engines enabling vertical take-off and landing. It will therefore be a hybrid of an aircraft and a multirotor. These vessels may have different masses. Polish law distinguishes between vessel weights of up to 0.25 kg, up to 0.9 kg, up to 4 kg and up to 25 kg. Vessels weighing more than 25 kg require a special permit for the operation issued by the President of the Civil Aviation Authority[5].

Virtually any air attack scenario can be implemented using UAVs. Their versatility is determined, among other things, by the following features:

1. They can be used in missions with a much higher risk of platform neutralisation than manned vessels. For this reason, drones are used in suicide missions where the price of success is the loss of the platform rather than the pilot.
2. They can perform missions controlled directly by the pilot, in automatic flight or in autonomous flight. Direct pilot control is by radio signal or by optical fibre. Automatic flight is when the route, flight parameters and tasks performed by the craft have been programmed by the pilot before take-off. Such flight takes place using sensors to assist the platform's on-board computer. In this type of flight, the pilot indicates the task, but the way the mission is performed depends on the AI algorithms implemented on the platform's on-board computer. In addition, the on-board computers, based on the sensor data, using AI algorithms, determine the value of the target and the potential losses of the enemy before deciding to attack and make a decision[6].
3. They have the ability to stay at one point in space for long periods of time, and thus can be used to observe a large area around

[5] *Act of 3 July 2002 – Aviation Law*; *Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft*; *Guideline No. 15/2023 of the President ofthe Civil Aviation Authority of 1 June 2023 on modalities of operations using unmanned aircraft systems in relation to the entry into force of the provisions of Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft*.

[6] J. Łukasiewicz, M. Piekarski, M. Kluczyński, *Bezpieczeństwo infrastruktury krytycznej wobec zagrożeń ze strony platform bezzałogowych* (Eng. Security of critical infrastructure in the face of threats from unmanned platforms), PTBN Report, vol. 2, Polskie Towarzystwo Bezpieczeństwa Narodowego 2021.

the hover point. Aircraft-type drones can carry explosive payloads over long distances and attack targets located far from the take-off point (i.e. where the pilot is). Confirmed distances flown by drones extend to several hundred kilometres[7].

4. They can be powered by electric motors, reciprocating internal combustion engines, and turbojet engines. Electric motors require a power source, i.e. a battery, fuel cell or generator powered by an internal combustion engine, but are relatively quiet. Internal combustion engines allow for missions over very long distances, while turbojet engines allow the platform to be accelerated to speeds unattainable by other propulsion systems.
5. They can be controlled using different frequencies, where communication is by radio directly between the flying platform and the ground station. Due to the possibility of jamming the radio signal, a mechanism for changing frequencies in flight has been developed. Long-range flights can be carried out using other aircraft carrying a device called a repeater, working as an intermediate station between the ground station and the platform. An unmanned aircraft can also be controlled using GSM communications. The prerequisite for a successful connection is that the flight region is saturated with a sufficient number of base transceiver stations (BTS). An increasingly popular and sometimes the only possible means of communication between the base station and the flying craft is satellite communication. It allows missions whose duration depends only on the energy resources required to power the aircraft's engine[8]. Where one of the methods of defending an attacked facility is to jam the radio frequencies on which the aircraft's connection to the ground station is implemented, a fibre-optic connection can be used. According to reports, the maximum length of fibre-optic

[7] *Timeline: UAE under drone, missile attacks,* Al Jazeera, 3.02.2022, https://www.aljazeera.com/news/2022/2/3/timeline-uae-drone-missile-attacks-houthis-yemen [accessed: 21.02.2025]; G. Faulconbridge, L. Kelly, *Ukrainian drone strikes trigger fires at major oil and gas facilities in Russia,* Reuters, 3.02.2025, https://www.reuters.com/world/europe/ukraines-drone-attack-sparks-fire-forces-flight-suspensions-several-russian-2025-02-03/ [accessed: 21.02.2025].

[8] C. Koulouris et al., *A Survey Study and Comparison of Drones Communication Systems,* in: *Flexible Electronics for Electric Vehicles. Proceedings of the 3rd International Conference, FlexEV 2022,* S.K. Goyal et al. (eds.), series: "Lecture Notes in Electrical Engineering", vol. 1065, Springer, Singapore. https://doi.org/10.1007/978-981-99-4795-9_33.

cable wound on a spool is currently 41 km[9]. Obviously, the need to carry a spool of fibre optics results in a reduction in the weight of the explosive charge. The advantage, however, is that the vessel moves in complete radio silence.

6. They can be built using many materials. The most common are injection moulded plastic, glass or carbon laminate moulded or cut with CNC milling machines, aluminium cut with CNC milling machines, 3D printing. Wood, plywood and ebonite are also used in the construction of drones.
7. They can carry any payload. Payloads can include measuring devices, image-recording devices and containers of explosives or chemicals. The use of hand grenades, RPG warheads and other explosives is observed in attacks. The ability to carry a payload has been provided by 3D printing.
8. Simple designs adapted for explosive flight and offering the possibility of observing the target of an attack (so-called FPV drones) can be built for as little as around USD 200[10]. More advanced designs and those intended for military use are much more expensive.
9. Acquiring the skills to control a platform is not complicated. Through the use of accelerometers and gyroscopes, as well as barometers and GPS receivers, systems that stabilise the platform, a pilot can acquire such skills in a matter of hours.

In view of the aforementioned characteristics of UAVs, the CI operator should consider the following scenarios and the consequences of an attack carried out with these devices when building their detection and neutralisation system:

1. Disruption of the operation of the facility or installation under attack by unauthorised overflight in the area of the facility. The consequences of an attack can be to cause distress to

[9] *Jam-Proof Fiber Optics for Drones: Revolutionizing Secure Communications,* Linden Photonics Inc, 22.08.2024, https://www.lindenphotonics.com/jam-proof-fiber-optics-for-drones-revolutionizing-secure-communications [accessed: 21.02.2025]; *Ukrainians Made an FPV With Fiber-Optic Cord Stretching For 41 km*, Defence Express, 26.01.2025, https://en.defence-ua.com/industries/ukrainians_made_an_fpv_with_fiber_optic_cord_stretching_for_41_km-13327.html [accessed: 21.02.2025].

[10] B. Wang, *Ukraine's One Million FPV Drones Is Outnumbered by 5 Million Russian Drones*, Next Big Future, 27.01.2024, https://www.nextbigfuture.com/2024/01/ukraines-one-million-fpv-drones-will-be-outnumbered-by-5-million-russian-drones.html [accessed: 21.02.2025].

personnel, disrupt their work, take them away from their routine activities, and involve government services in efforts to identify the perpetrator of the attack[11].

2. Espionage activities. The consequences of such an attack may include the identification of: the structural features of the facility or the industrial installations used in the facility, the manufacturer of the equipment used in the technological processes, the procedures in place at the facility under attack, the identity of the employees and the methods of communication between the employees working at the facility[12].
3. A kinetic impact, breaking a platform, dropping a load that mechanically damages equipment and installations and then stops their operation, hanging electrically conductive elements such as wires, carbon fibres or carbon dust on electrical equipment. The consequences of an attack can be damage to installations, causing injury to people, causing panic, and short-circuiting the electrical system supplying the facility or installation[13].
4. Carrying an explosive charge and causing it to explode. The consequences of an attack can be: loss of life or limb to workers, damage to installations causing a long term interruption to the operation of the facility, panic, stress and, in the long term, social unrest[14].
5. Transfer of chemical, biological, radiological or other irritant weapons. The consequences of an attack may be: the long-term contamination of the area of the facility preventing its operation, damage to installations required in the technological process,

[11] *It is still unclear whose drone is blocking 6 flights at Sofia Airport*, Fakti.bg, 9.02.2025, https://fakti.bg/en/bulgaria/948414-it-is-still-unclear-whose-drone-is-blocking-6-flights-at-sofia-airport [accessed: 21.02.2025].

[12] *Sweden drones: Sightings reported over nuclear plants and palace*, BBC, 18.01.2022, https://www.bbc.com/news/world-europe-60035446 [accessed: 21.02.2025].

[13] S. Lyngaas, *Drone at Pennsylvania electric substation was first to 'specifically target energy infrastructure', according to federal law enforcement bulletin*, CNN, 4.11.2021, https://edition.cnn.com/2021/11/04/politics/drone-pennsylvania-electric-substation/index.html [accessed: 21.02.2025]; B. Barrett, *A Drone Tried to Disrupt the Power Grid. It Won't Be the Last*, Wired, 5.11.2021, https://www.wired.com/story/drone-attack-power-substation-threat/ [accessed: 21.02.2025].

[14] G. Faulconbridge, L. Kelly, *Ukrainian drone strikes trigger fires*...

causing fires, including in the area surrounding the protected facility[15].

6. Smuggling of unauthorised loads both into and out of the facility outside the fence. The consequence of smuggling may be the appearance of firearms, explosives, electronic warfare agents, drugs etc. on the premises[16]. Smuggling out of the facility may result in loss of control over classified information that must not be transferred off-site, loss of protected chemical, biological or nuclear agents, etc.

Legislative changes to the protection of critical infrastructure from unmanned aerial vehicles

The existing legislation in Poland so far has practically failed to take into account the possibility of combating unmanned aircraft, even when they posed a threat to protected facilities, air traffic, health or human life. In the world, the consequence of the lack of proper regulations was the overflight of unmanned aircraft over protected objects and even flights on collision courses with manned aircraft[17]. There have also been isolated incidents of unmanned platforms being used in attacks on people[18]. Such situations, the war in Ukraine, daily reports of attacks on CI facilities around the world, as well as hybrid actions in the Baltic Sea, have shown that ensuring the security of CI in Poland, for which UAVs are a source of threat, requires serious legal changes.

[15] *Drone 'containing radiation' lands on roof of Japanese PM's office*, The Guardian, 22.04.2015, https://www.theguardian.com/world/2015/apr/22/drone-with-radiation-sign-lands-on-roof-of-japanese-prime-ministers-office [accessed: 21.02.2025].

[16] *Cheap and They Don't Snitch: Drones Are the New Drug Mules*, RUSI, 5.01.2024, https://www.rusi.org/news-and-comment/in-the-news/cheap-and-they-dont-snitch-drones-are-new-drug-mules [accessed: 21.02.2025].

[17] S. McKenzie, G. Mezzofiore, *Police hunt drone pilots in unprecedented Gatwick Airport disruption*, CNN, 20.12.2018, https://edition.cnn.com/2018/12/20/uk/gatwick-airport-drones-gbr-intl/index.html [accessed: 21.02.2025]; *Drones paralyzed Stockholm-Arlanda Airport*, Kronen Zeitung, 9.09.2024, https://www.krone.at/3519874 [accessed: 21.02.2025].

[18] *Venezuela President Maduro survives 'drone assassination attempt'*, BBC, 5.08.2018, https://www.bbc.com/news/world-latin-america-45073385 [accessed: 21.02.2025].

The new provisions enshrined in the *Act amending the Aviation Law and certain other acts*[19] are the response to these threats. The draft was received by the Polish Parliament on 24 November 2024[20]. On 24 January 2025, it was forwarded to the President of Poland, who signed the law on 6 February 2025. It implements those provisions of EU law that relate to UAVs[21]. The Act has put in order the previous legal status on the basis of which unmanned aircraft flights were performed in Poland. A novelty in relation to the current Act – the Aviation Law is the introduction of Part VIa entirely dedicated to unmanned aircraft. It contains, inter alia, Chapter 2, on geographical zones for unmanned aircraft, and Chapter 6, relating to the prevention of unlawful operations using an unmanned aircraft system.

Airspace designated for the operation of aircraft in accordance with the provisions of the Aviation Law is divided into controlled space and uncontrolled space[22]. The structure of the space is defined, by regulation, by the minister responsible for transport, but in consultation with the minister of national defence and taking into account the rules arising from regulations and international agreements. According to the ordinance of the Minister of Infrastructure of 27 December 2018[23], a controlled space is one in which an air traffic control service is provided to all aircraft, based on the classification of the International Civil Aviation Organization. This service guarantees separation between aircraft, an alerting service and a flight information service. In uncontrolled space, only alerting service and flight information service are provided, and the separation between aircraft and other aircraft flying in the uncontrolled area is ensured by the aircraft pilot himself. In Poland, controlled space extends from FL095 to FL660 (Flight Level 660 – flight level of 66000 feet), while uncontrolled space extends from the ground to FL095 (Flight Level 095 – flight level of 9500 feet). Within controlled and uncontrolled space, fixed and flexible

[19] *Act of 24 January 2025 amending the Aviation Law and certain other acts.*

[20] *Government draft Act amending the Aviation Law and certain other acts*, print no. 810, https://www.sejm.gov.pl/sejm10.nsf/PrzebiegProc.xsp?nr=810 [accessed: 21.02.2025].

[21] *Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems*; *Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft*.

[22] Article 121(5) of the *Act of 3 July 2002 – Aviation Law*.

[23] *Regulation of the Minister of Infrastructure of 27 December 2018 on the structure of Polish airspace and the detailed conditions and use of that space*.

airspace elements are further delimited to ensure flight safety, more efficient use of airspace and optimised air traffic management. Fixed elements are those whose horizontal and vertical boundaries are defined and unchangeable. These include, for example: Airways (AWY), Control Zones (CTR), Prohibited Area (P). Flexible elements, separated only for a limited period of time, are e.g. Temporary Selected Areas (TSA) or Aerodrome Traffic Zones (ATZ).

The fixed and flexible elements listed were developed at a time when unmanned aviation was not widespread and the flight rules applicable to these elements were adapted to manned aviation. The rapid development of unmanned aviation made it necessary to structure the airspace for unmanned operations. In view of the lack of appropriate provisions in laws and regulations, under the guidelines of the President of the Civil Aviation Authority, the designation of so-called geographical zones for unmanned aircraft systems began[24]. The amendment to the Aviation Law allowed the content of these guidelines to be written down in Chapter 2 of the act. Under the new provisions, the Polish Air Navigation Services Agency (hereinafter: the Agency) is responsible for designating the geographical zone, which determines the period of validity of the zone, the area of the geographical zone and the conditions under which flights by UAVs in the zone must be performed[25].

According to the new regulations, an application for the designation of a geographical zone may be submitted by an authorised entity, which is:

1) public administration body, a body of the Armed Forces of the Republic of Poland, the chairman of the State Commission on Aircraft Accidents Investigation, the chairman of the Commission for Investigation of State Aviation Accidents, the Director General of the State Forests National Forest Holding, an entity authorised to carry out water rescue, an entity authorised to carry out mountain rescue and the director of the Government Centre for Security – in the event of the need to secure airspace in order to carry out statutory tasks;
2) manager of a CI, including aviation, maritime, rail or energy infrastructure, or a mining site, where it is necessary to secure airspace in order to discharge the responsibilities of that manager;

[24] *Guideline No. 17/2023 of the President of the Civil Aviation Authority of 6 June 2023 on the designation of geographical zones for unmanned aircraft systems*. These guidelines were updated in a document dated 21 February 2025.

[25] Article 156h(13) of the *Act of 3 July 2002 – Aviation Law*.

3) organiser of exercises, training, competitions, air shows or occasional flights, when airspace has to be secured for flights during exercises, training, competitions, air shows or occasional flights;
4) operator of an unmanned aircraft system intending to conduct an operation in the 'special' category, where the need for a geographical zone designation results from the authorisation of the operation, the LUC certificate, the standard scenario or the national standard scenario;
5) recognised provider of practical training and assessment of the practical skills of an unmanned aircraft pilot for operations in the 'specific' category and a manufacturer of unmanned aircraft systems[26].

The above provisions of the amended law allow the CI operator to designate a drone geographical zone over the area where the protected CI facility is located.

The types of geographical zones, detailed conditions and the manner of using them will be specified by the minister responsible for transport by means of a regulation. Currently, the following types of geographical zones are distinguished in Poland:

1) DRA-P – a prohibited zone for unmanned aircraft systems, in which operations using unmanned aircraft systems may not be carried out, except under conditions specified by the Agency, the General Commander of the Armed Forces, the Operational Commander of the Armed Forces, the Commander-in-Chief of the Military Police, the Head of the Internal Security Agency, the Head of the Foreign Intelligence Agency, the Head of the Central Anticorruption Bureau, the Head of the Military Counterintelligence Service, the Head of the Military Intelligence Service, the Commander-in-Chief of the Police, the Commander-in-Chief of the Border Guard, the General Director of the Prison Service, the Head of the National Revenue Administration, the Commander-in-Chief of the State Protection Service or the Commander-in-Chief of the State Fire Service – under the conditions specified by the Agency;
2) DRA-R – a restricted zone for unmanned aircraft systems, in which operations using unmanned aircraft systems may be carried out with the consent and under conditions specified by the Agency

[26] Article 156h(4) of the *Act of 3 July 2002 – Aviation Law*.

or the authorised entity at the request of which the geographical zone has been designated, including:

a) DRA-RH – a restricted zone for unmanned aircraft systems with a high probability of approval by the geographical zone manager to carry out the operation,
b) DRA-RM – a restricted zone for unmanned aircraft systems with a medium probability of obtaining approval by the geographical zone manager to carry out the operation,
c) DRA-RL – a restricted zone for unmanned aircraft systems with a low probability of obtaining approval by the geographical zone manager to carry out the operation;

3) DRA-T – a restricted zone for unmanned aircraft systems in which operations with unmanned aircraft systems may only be carried out with unmanned aircraft systems meeting the technical requirements specified by the Agency and under conditions specified by the Agency, for the DRA-T zone, additional conditions for operations are allowed, including the obligation to obtain the approval of the geographical zone manager;
4) DRA-I – information zone for unmanned aircraft, containing information necessary to ensure safe operations using unmanned aircraft systems, including navigational warnings[27].

The amended Aviation Law also introduces provisions aimed at enabling the destruction, immobilisation or takeover of an unmanned aircraft in cases where the pilot performs a flight operation in such a way that the course of the operation or the operation of the unmanned aircraft:

1) threatens or is likely to threaten the life or health of humans or animals,
2) poses or is likely to pose a threat to protected objects, equipment or areas,
3) disrupts or is likely to disrupt a mass event or endangers the safety of its participants,
4) creates or may create a reasonable suspicion that it may be used as a means of a terrorist attack,
5) creates or is likely to create a risk to the safety of air traffic, aircraft or the life or health of the crew or passengers on board,

[27] *Guideline No. 4/2025 of the President of the Civil Aviation Authority of 21 February 2025 on the designation of geographical zones for unmanned aircraft systems.*

6) obstructs or is likely to obstruct air traffic or causes or is likely to cause its interruption or restriction[28].

An unmanned aircraft may also be destroyed, immobilised or its flight may be overtaken if, contrary to the prohibition, it performs an operation in the geographical zone established over: protected facilities of the Polish Armed Forces and organisational units subordinate to the Minister of National Defence or supervised by him or facilities, equipment or areas important for the security or defence of the state, public security or the inviolability of the state border[29].

The aforementioned provisions of the amended law are revolutionary with regard to the security of CI facilities. Until the amendment, the law allowed for the detection of UAVs, but did not give the operator the tools to neutralise vessels infringing the geographical zone designated over the facilities protected by the zone. Due to the lack of a legal basis and, above all, for fear of liability for potential losses caused by the neutralisation of an unmanned aircraft, many CI operators have not installed systems to detect and neutralise these vessels. The amended law unambiguously identifies the pilot or operator of the aircraft performing the operation in violation of the law as responsible for the damage caused by the neutralisation of the aircraft[30].

When an unmanned aircraft:

- threatens or is likely to threaten the life or health of humans or animals,
- poses or is likely to pose a threat to protected facilities, equipment or areas,
- creates or may create a reasonable suspicion that it may be used as a means of a terrorist attack,
- poses or is likely to pose a threat to the safety of air traffic, the aircraft or the life or health of the crew or passengers on board,
- obstructs or is likely to obstruct air traffic or causes or is likely to cause its interruption or restriction,

officers of the Internal Security Agency, the Foreign Intelligence Agency, the Military Counterintelligence Service, the Military Intelligence Service, the Central Anticorruption Bureau, the Police, the Border Guard, the State

[28] Article 156ze(1), point 1 of the *Act of 3 July 2002 – Aviation Law*.

[29] Article 156ze(1), point 2 of the *Act of 3 July 2002 – Aviation Law*.

[30] Article 156ze(4) of the *Act of 3 July 2002 – Aviation Law*.

Protection Service, the Customs and Tax Service, the Prison Service, the Marshal Guard, inspectors of the Office for Internal Oversight, professional soldiers appointed to service positions in the Military Counterintelligence Service or the Military Intelligence Service, soldiers of the Military Police and the Armed Forces of the Republic of Poland, employees of airport security services, forest guards, security employees of specialised armed protection formations, as well as employees of internal protection services operating on the territory of organisational units subordinated to the Minister of National Defence or supervised by him are entitled to destroy, immobilise or take control of such vessel[31].

The amended Act provides penalties for violations of the regulations on operations with unmanned aircraft. In Part XIa – Administrative fines – provisions have been added to allow a penalty to be imposed on anyone who carries out operations using an unmanned aircraft system contrary to the conditions for carrying out operations in a given geographical zone. The amount of such penalty is PLN 10 000 for each infringement.

Another important revision is the amendment of the Act of 24 May 2013 on means of direct coercion and firearms[32]. It extends the catalogue of direct coercive measures to include the destruction or immobilisation of an unmanned aircraft or taking control of its flight[33]. The law has also been supplemented with an indication of the means of neutralising the UAV, which include:

1) a device that uses or interferes with radio waves,
2) an incapacitating net,
3) other UAVs,
4) non-penetrating projectiles or other objects propelled by means of devices designed for that purpose and by firearms and airsoft weapons,
5) devices emitting a cumulative beam of energy or electromagnetic waves[34].

The list of measures includes all currently known methods of neutralising UAVs.

[31] Article 156ze(2) of the *Act of 3 July 2002 – Aviation Law.*

[32] *Act of 24 May 2013 on means of direct coercion and firearms.*

[33] Ibid., Article 11.

[34] Ibid., Article 33a(2).

Recommendations of the Government Centre for Security on assessing the effectiveness of unmanned aircraft detection and neutralisation systems

With reports of unmanned platforms being used to paralyse the operation of technical systems responsible for the continuity of CI operations[35], disturbing facility staff[36] or even attacks with explosives[37], CI operators should consider building detection and neutralisation systems for drones.

The process of building a UAV detection and neutralisation system begins with a risk analysis of the system or facility for which the unmanned platforms are a threat source. If the CI operator considers that the system or facility it is protecting is vulnerable to attack, then building a detection and neutralisation system is essential.

Detection systems are made up of multiple devices using different methods to detect unmanned platforms[38]. The simplest and seemingly most widely used detection method is the detection of communication between the flying platform and the ground station. It is versatile as both fixed and mobile detection devices can be used within this framework. Advanced devices using AI algorithms can determine the model of the aircraft based on the measurement of the characteristics of the communication signal[39]. These easily constructed devices work on the principle of an indicator that emits an audible signal when a flying vessel is detected. Their disadvantage is the inability to detect unmanned vessels flying in radio silence, for example those controlled by fibre optic cable, and the inability to detect platforms whose communications are on frequencies not supported by the detection device.

Another detection method uses radar devices. It has the advantage of a wide radar range – its detection distance far exceeds the distances at which an unmanned aircraft can be detected by other methods. However,

[35] *Drones paralyzed Stockholm-Arlanda Airport...*; S. Lyngaas, *Drone at Pennsylvania electric substation...*

[36] H. Altman, *Nuclear Power Plants Report Massive Uptick In Drone Sightings*, The Warzone, 21.12.2024, https://www.twz.com/news-features/massive-uptick-in-official-drone-sightings-by-nuclear-power-plants [accessed: 21.02.2025].

[37] L. Kelly, *Ukrainian drone strikes trigger fires...*

[38] J. Łukasiewicz, M. Piekarski, M. Kluczyński, *Bezpieczeństwo infrastruktury krytycznej...*

[39] M.F. Al-Sa'd et al., *RF-based drone detection and identification using deep learning approaches: An initiative towards a large open-source drone database*, "Future Generation Computer Systems" 2019, vol. 100, pp. 86–97. https://doi.org/10.1016/j.future.2019.05.007.

the probability of detecting an aircraft depends on several factors, including the size of the object being detected and the altitude at which it is moving[40]. Modern radar systems aided by AI algorithms can determine whether the tracked object is an unmanned platform or a bird. The method described also has the advantage of being able to detect the object regardless of the time of day or night. The disadvantage of radar detection is certainly the high cost of the device and the inability to detect a flying object if it is hiding behind terrain obstacles or flying very low to the ground.

The acoustic method is increasingly used[41]. The cost of an acoustic detector is lower than a radar detector and, more importantly, it is passive, i.e. it does not emit a signal in any form to make a detection. This method is becoming increasingly popular for drone detection systems in Ukraine, where the large platforms used to carry high explosive loads are powered by noisy internal combustion engines. The disadvantage of the acoustic method may be ineffective detection in a location where there are other noise sources than just the unmanned platform.

The final detection method is to analyse the image recorded by a camera operating in visible light or infrared[42]. Such a camera is equipped with AI algorithms to recognise the shape of a flying object. Infrared cameras analyse its temperature, which makes it possible to distinguish between the unmanned platform and the birds. The disadvantage of cameras operating in the visible area is the inability to record images in low-light conditions, such as at night. The disadvantage of infrared cameras, on the other hand, is the inability to detect the object when it is equipped with thermal insulators.

All the described methods used in the construction of the detection system allow for the detection of unmanned platforms in various conditions. The method for assessing the effectiveness of this system is described in a document prepared by the Government Centre for Security

[40] M. Ezuma et al., *Comparative Analysis of Radar Cross Section Based UAV Classification Techniques*, preprint, https://arxiv.org/abs/2112.09774 [accessed: 21.02.2025]. https://doi.org/10.48550/arXiv.2112.09774.

[41] H. Altman, T. Rogoway, *Ukraine's Acoustic Drone Detection Network Eyed By U.S. As Low-Cost Air Defense Option*, The Warzone, 24.07.2024, https://www.twz.com/air/ukraines-acoustic-drone-detection-network-eyed-by-u-s-as-low-cost-air-defense-option [accessed: 21.02.2025].

[42] Y. Wu, Y. Sui, G. Wang, *Vision-Based Real-Time Aerial Object Localization and Tracking for UAV Sensing System*, "IEEE Access" 2017, vol. 5, pp. 23969–23978. https://doi.org/10.1109/ACCESS.2017.2764419.

as an annex to the National Critical Infrastructure Protection Program 2023 (NPOIK)[43]. The method involves testing the probability of detection by individual devices in the system. This probability is determined from the counts of effective detections per 100 trials. These trials must take place under different conditions, i.e. the probability of detection for a given location under different weather conditions, under conditions of external sources of electromagnetic radiation, for different types of UAVs, for different attack scenarios, for different competences of security personnel is examined. Knowing the probability of detection of each device under given conditions, the total probability of detection by the entire system can be determined using the formula:

$$P_{CAŁK\_D} = 1 - (1 - P_{1D})(1 - P_{2D})(1 - P_{3D})(1 - P_{4D}) \ldots (1 - P_{ND})$$

in which:

$P_{CAŁK\_D}$ – is the probability of detection by the whole system,
P_{1D} – is the probability of detection by the first detection device,
P_{2D} – is the probability of detection by the second detection device,
P_{3D} – is the probability of detection by the third detection device,
P_{ND} – is the probability of detection by the nth detection device.

The task of the CI operator is to build a detection system such that the probability value $P_{CAŁK\_D}$ is higher than the threshold value assumed by the operator.

The construction of drone neutralisation systems also uses devices that operate on different principles to increase the likelihood of neutralisation. One of its most popular methods is the jamming of the communication signal between unmanned platform and ground station. The jamming is done by emitting an electromagnetic wave in the direction of the flying platform at the same frequency as that used for communication. The disadvantage of this solution is the increasingly common hopping mechanism, which involves changing the frequency of communication between the platform and the ground station during flight. The jamming device must therefore emit waves at different frequencies to jam the communication. Such

[43] *Standards for ensuring the smooth functioning of critical infrastructure – good practices and recommendations*, Annex 1 to the National Critical Infrastructure Protection Program, Government Centre for Security (RCB), 2023. The text of the Annex is available at: https://www.gov.pl/web/rcb-en/national-critical-infrastructure-protection-program.

a device is not effective against an unmanned platform flying in radio silence or in automatic or autonomous mode.

Another method is to jam or spoof the satellite navigation signal[44], which will result in the unmanned platform getting lost in the airspace or flying the platform to the location indicated by the falsified satellite navigation signal. This solution will prove ineffective if the unmanned platform uses counting navigation equipment, known as inertial navigation. In this case, the unmanned platform navigates on the basis of calculations, correcting its geographical position by periodic position readings from satellites.

A third method is the use of net systems that can be fired from special devices called *net guns*, which security personnel are equipped with, or devices carried by unmanned aircraft operated by security personnel[45]. The disadvantage of this method is that the shot must be fired at close range from the attacking platform.

Another method of neutralisation is to destroy the UAV by emitting a high-energy electromagnetic pulse in its direction[46]. Such a pulse destroys the semiconductor components of the electronics mounted on the platform. The disadvantage of this solution is that sensitive electronic components can be placed in what is known as a Faraday cage, a package that isolates electronic devices from the effects of external electromagnetic fields.

Laser systems are increasingly being used to combat unmanned systems. Lasers can be used as light sources that, by shining directly into the camera lens of the unmanned platform, prevent the pilot from controlling it properly. Lasers are also increasingly used as a device that physically destroys the illuminated platform by burning it[47]. Laser systems

[44] M. Sahmoudi, M.G. Amin, *Robust tracking of weak GPS signals in multipath and jamming environments*, "Signal Processing" 2009, vol. 89, no. 7, pp. 1320–1333. https://doi.org/10.1016/j.sigpro.2009.01.001.

[45] D. Hambling, *Webslingers: How Net-Launching Drones Are Downing Russian Quadcopters*, Forbes, 12.12.2024, https://www.forbes.com/sites/davidhambling/2024/11/12/webslingers-how-net-launching-drones-are-downing-russian-quadcopters/ [accessed: 21.02.2025].

[46] O.D. Razooqi, A.H. Ali, *Drones neutralized by utilize electromagnetic pulse (EMP) system*, in: *2022 5th International Conference on Engineering Technology and its Applications (IICETA)*, Al-Najaf 2022, pp. 487–492. https://doi.org/10.1109/IICETA54559.2022.9888673.

[47] J. Saballa, *Ukraine Announces Successful Use of First Laser Weapon on Battlefield*, The Defense Post, 6.02.2025, https://thedefensepost.com/2025/02/06/ukraine-laser-weapon-battlefield/ [accessed: 21.02.2025].

are not popular because they require large and efficient energy sources, and their effectiveness is highly dependent on air transparency[48].

None of the described methods guarantees neutralisation, so, as mentioned, systems using different methods should be built. A proposal on how to evaluate the effectiveness of a system to neutralise unmanned platforms is described in the aforementioned annex to the NPOIK 2023[49]. The method involves testing the probability of neutralisation using individual devices of the system. This probability is determined on the basis of the counts of successful neutralisations per 100 trials. These trials must take place under different conditions, i.e. the probability of neutralisation is tested for a given location under different weather conditions, for different types of UAVs, for different attack scenarios, for different competences of security personnel. Knowing the probability of neutralisation of each device of the system under given conditions, the total probability of neutralisation by the whole system can be determined using the formula:

$$P_{CAŁK\_N} = 1 - (1 - P_{1N})(1 - P_{2N})(1 - P_{3N})(1 - P_{4N}) \ldots (1 - P_{NN})$$

where:

$P_{CAŁK\_N}$ – is the probability of neutralisation by the whole system,
P_{1N} – is the probability of neutralisation by the first neutralisation device,
P_{2N} – is the probability of neutralisation by the second neutralisation device,
P_{3N} – is the probability of neutralisation by the third neutralisation device,
P_{NN} – is the probability of neutralisation by the nth neutralisation device.

The task of the CI operator is to build the neutralisation system in such a way that the probability value $P_{CAŁK\_N}$ is higher than the minimum threshold value assumed by the operator.

[48] R. Ceder, *US Navy hits drone with HELIOS laser in successful test*, Navy Times, 4.02.2025, https://www.navytimes.com/news/your-navy/2025/02/04/us-navy-hits-drone-with-helios-laser-in-successful-test/ [accessed: 21.02.2025]; M. Knight, *Ukraine says it has a laser that can shoot down aircraft a mile away. It's called 'Tryzub'*, CNN, 18.12.2024, https://edition.cnn.com/2024/12/18/europe/ukrainian-tryzub-laser-weapon-intl-latam/index.html [accessed: 21.02.2025].

[49] *Standards to ensure smooth functioning...*

Summary

The amendment to the Polish Act – Aviation Law has been eagerly awaited by CI operators. It provides them with ample opportunities and a formal legal basis to combat drones that unauthorised violate the geographical zone designated over a CI facility. The new legislation clearly identifies the pilot of an unmanned platform in breach of the flight rules as the person who bears the consequences of a potential drone fall resulting in damage. The penalties introduced in this respect can be assessed as very severe. In addition, the amendment to the Act on direct coercive measures and firearms expands the catalogue of such measures to include devices that can be used to combat unmanned platforms. The amendment to the Aviation Law in question should be supplemented by an amendment to the Act on crisis management to oblige CI operators to conduct risk analyses of threats to facilities and, consequently, to build detection and neutralisation systems for unmanned aircraft.

In view of the rapid development of unmanned technology, the emergence of drone munitions, the increasingly widespread acquisition of UAV piloting skills, both EU institutions and Member States should encourage research institutions, laboratories, technology centres and private investors to invest in the research and development of modern detection and neutralisation systems for unmanned platforms. Based on the observation of the armed conflict in Ukraine, it can be concluded that current detection and neutralisation systems do not guarantee the security of protected facilities.

The technological gap between the ability of UAVs to attack CI facilities and the systems to detect and neutralise them is regularly widening. The same conclusion can be reached after comparing the cost of acquiring an unmanned aircraft capable of attacking a CI facility with the cost of acquiring, operating and servicing an anti-drone system that reduces the risk of attack to an acceptable level for the CI operator. This gap must not be allowed to widen. Increasing the resilience of CI facilities to attacks using unmanned aircraft systems depends on the actions of CI operators, who have received the legal and organisational framework that has been advocated for years.

Bibliography

Al-Sa'd M.F., Al-Ali A., Mohamed A., Khattab T., Erbad A., *RF-based drone detection and identification using deep learning approaches: An initiative towards a large open-source drone database*, "Future Generation Computer Systems" 2019, vol. 100, pp. 86–97. https://doi.org/10.1016/j.future.2019.05.007.

Ezuma M., Anjinappa C.K., Semkin V., Guvenc I., *Comparative Analysis of Radar Cross Section Based UAV Classification Techniques*, preprint, https://arxiv.org/abs/2112.09774 [accessed: 21.02.2025]. https://doi.org/10.48550/arXiv.2112.09774.

Koulouris C., Dimitrios P., Al-Darraji I., Tsaramirsis G., Khadidos A.O., Khadidos A.O., Papageorgasi P., *A Survey Study and Comparison of Drones Communication Systems*, in: *Flexible Electronics for Electric Vehicles. Proceedings of the 3rd International Conference, FlexEV 2022*, S.K. Goyal, D.K. Palwalia, R. Tiwari, Y. Gupta (eds.), series: "Lecture Notes in Electrical Engineering", vol. 1065. Springer, Singapore. https://doi.org/10.1007/978-981-99-4795-9_33.

Łukasiewicz J., Piekarski M., Kluczyński M., *Bezpieczeństwo infrastruktury krytycznej wobec zagrożeń ze strony platform bezzałogowych* (Eng. Security of critical infrastructure in the face of threats from unmanned platforms), PTBN Report, vol. 2, Polskie Towarzystwo Bezpieczeństwa Narodowego 2021.

Razooqi O.D., Ali A.H., *Drones neutralized by utilize electromagnetic pulse (EMP) system*, in: *2022 5th International Conference on Engineering Technology and its Applications (IICETA)*, Al-Najaf 2022, pp. 487–492. https://doi.org/10.1109/IICETA54559.2022.9888673.

Sahmoudi M., Amin M.G., *Robust tracking of weak GPS signals in multipath and jamming environments*, "Signal Processing" 2009, vol. 89, no. 7, pp. 1320–1333. https://doi.org/10.1016/j.sigpro.2009.01.001.

Standards for ensuring the smooth functioning of critical infrastructure – good practices and recommendations, Annex 1 to the National Critical Infrastructure Protection Program, Government Centre for Security (RCB), 2023.

Szlachter D., *Terrorism in Poland and trends in its development. Survey results (summary report)*, "Terrorism – Studies, Analyses, Prevention" 2022, no. 2, pp. 335–363. https://doi.org/10.4467/27204383TER.22.029.16349.

Wu Y., Sui Y., Wang G., *Vision-Based Real-Time Aerial Object Localization and Tracking for UAV Sensing System*, "IEEE Access" 2017, vol. 5, pp. 23969–23978. https://doi.org/10.1109/ACCESS.2017.2764419.

Internet sources

Altman H., *Nuclear Power Plants Report Massive Uptick In Drone Sightings*, The Warzone, 21.12.2024, https://www.twz.com/news-features/massive-uptick-in-official-drone-sightings-by-nuclear-power-plants [accessed: 21.02.2025].

Altman H., Rogoway T., *Ukraine's Acoustic Drone Detection Network Eyed By U.S. As Low-Cost Air Defense Option*, The Warzone, 24.07.2024, https://www.twz.com/air/ukraines-acoustic-drone-detection-network-eyed-by-u-s-as-low-cost-air-defense-option [accessed: 21.02.2025].

Barrett B., *A Drone Tried to Disrupt the Power Grid. It Won't Be the Last*, Wired, 5.11.2021, https://www.wired.com/story/drone-attack-power-substation-threat/ [accessed: 21.02.2025].

Ceder R., *US Navy hits drone with HELIOS laser in successful test*, Navy Times, 4.02.2025, https://www.navytimes.com/news/your-navy/2025/02/04/us-navy-hits-drone-with-helios-laser-in-successful-test/ [accessed: 21.02.2025].

Cheap and They Don't Snitch: Drones Are the New Drug Mules, RUSI, 5.01.2024, https://www.rusi.org/news-and-comment/in-the-news/cheap-and-they-dont-snitch-drones-are-new-drug-mules [accessed: 21.02.2025].

Drone 'containing radiation' lands on roof of Japanese PM's office, The Guardian, 22.04.2015, https://www.theguardian.com/world/2015/apr/22/drone-with-radiation-sign-lands-on-roof-of-japanese-prime-ministers-office [accessed: 21.02.2025].

Faulconbridge G., Kelly L., *Ukrainian drone strikes trigger fires at major oil and gas facilities in Russia*, Reuters, 3.02.2025, https://www.reuters.com/world/europe/ukraines-drone-attack-sparks-fire-forces-flight-suspensions-several-russian-2025-02-03/ [accessed: 21.02.2025].

Hambling D., *Webslingers: How Net-Launching Drones Are Downing Russian Quadcopters*, Forbes, 12.12.2024, https://www.forbes.com/sites/davidhambling/2024/11/12/webslingers-how-net-launching-drones-are-downing-russian-quadcopters/ [accessed: 21.02.2025].

It is still unclear whose drone is blocking 6 flights at Sofia Airport, Fakti.bg, 9.02.2025, https://fakti.bg/en/bulgaria/948414-it-is-still-unclear-whose-drone-is-blocking-6-flights-at-sofia-airport [accessed: 21.02.2025].

Jam-Proof Fiber Optics for Drones: Revolutionizing Secure Communications, Linden Photonics Inc, 22.08.2024, https://www.lindenphotonics.com/jam-proof-fiber-optics-for-drones-revolutionizing-secure-communications [accessed: 21.02.2025].

Knight M., *Ukraine says it has a laser that can shoot down aircraft a mile away. It's called 'Tryzub'*, CNN, 18.12.2024, https://edition.cnn.com/2024/12/18/europe/ukrainian-tryzub-laser-weapon-intl-latam/index.html [accessed: 21.02.2025].

Lyngaas S., *Drone at Pennsylvania electric substation was first to 'specifically target energy infrastructure', according to federal law enforcement bulletin*, CNN, 4.11.2021, https://edition.cnn.com/2021/11/04/politics/drone-pennsylvania-electric-substation/index.html [accessed: 21.02.2025].

McKenzie S., Mezzofiore G., *Police hunt drone pilots in unprecedented Gatwick Airport disruption*, CNN, 20.12.2018, https://edition.cnn.com/2018/12/20/uk/gatwick-airport-drones-gbr-intl/index.html [accessed: 21.02.2025].

Saballa J., *Ukraine Announces Successful Use of First Laser Weapon on Battlefield*, *The Defense Post*, 6.02.2025, https://thedefensepost.com/2025/02/06/ukraine-laser-weapon-battlefield/ [accessed: 21.02.2025].

Sweden drones: Sightings reported over nuclear plants and palace, BBC, 18.01.2022, https://www.bbc.com/news/world-europe-60035446 [accessed: 21.02.2025].

Timeline: UAE under drone, missile attacks, Al Jazeera, 3.02.2022, https://www.aljazeera.com/news/2022/2/3/timeline-uae-drone-missile-attacks-houthis-yemen [accessed: 21.02.2025].

Ukrainians Made an FPV With Fiber-Optic Cord Stretching For 41 km, Defence Express, 26.01.2025, https://en.defence-ua.com/industries/ukrainians_made_an_fpv_with_fiber_optic_cord_stretching_for_41_km-13327.html [accessed: 21.02.2025].

Venezuela President Maduro survives 'drone assassination attempt', BBC, 5.08.2018, https://www.bbc.com/news/world-latin-america-45073385 [accessed: 21.02.2025].

Wang B., *Ukraine's One Million FPV Drones Is Outnumbered by 5 Million Russian Drones*, Next Big Future, 27.01.2024, https://www.nextbigfuture.com/2024/01/ukraines-one-million-fpv-drones-will-be-outnumbered-by-5-million-russian-drones.html [accessed: 21.02.2025].

Legal acts

Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft (EU Official Journal L 152/45 of 11.06.2019).

Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems (EU Official Journal L 152/1 of 11.06.2019).

Act of 24 January 2025 amending the Aviation Law and certain other acts (Journal of Laws of 2025, item 179).

Act of 24 May 2013 on means of direct coercion and firearms (Journal of Laws of 2024, item 383, as amended).

Act of 26 April 2007 on crisis management (Journal of Laws of 2023, item 122, as amended).

Act of 3 July 2002 – Aviation Law (Journal of Laws of 2023, item 2110, as amended).

Regulation of the Minister of Infrastructure of 27 December 2018 on the structure of Polish airspace and the detailed conditions and use of that space (Journal of Laws of 2019, item 619).

Guideline No. 4/2025 of the President of the Civil Aviation Authority of 21 February 2025 on the designation of geographical zones for unmanned aircraft systems.

Guideline No. 17/2023 of the President of the Civil Aviation Authority of 6 June 2023 on the designation of geographical zones for unmanned aircraft systems (Official Journal of the CAA of 2023, item 42).

Guideline No. 15/2023 of the President of the Civil Aviation Authority of 1 June 2023 on modalities of operations using unmanned aircraft systems in view of the entry into force of the provisions of Commission Implementing Regulation (EU) No. 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft (Official Journal of the CAA of 2023, item 39).

Other documents

Government draft Act amending the Aviation Law and certain other acts, print no. 810, https://www.sejm.gov.pl/sejm10.nsf/PrzebiegProc.xsp?nr=810 [accessed: 21.02.2025].

Jędrzej Łukasiewicz, PhD

Doctor of Physical Sciences. He is a former employee of the Poznań University of Technology, where he was employed as an assistant professor. Designer and pilot of unmanned aerial vehicles. Instructor at the drone pilot training centre of the Poznań University of Technology. He specialises in the security of critical infrastructure facilities for which unmanned aerial vehicles are a source of threats. Author of a method for assessing the effectiveness of detection and neutralisation systems for unmanned aerial vehicles. This method is described in Annex 1 to the National Critical Infrastructure Protection Program entitled *Standards for ensuring the efficient functioning of critical infrastructure - good practices and recommendations*. Author of scientific articles published in international journals. Participant in the work of departmental teams supporting the state administration in increasing the state's resilience to hybrid threats.

Contact: jedrzej.lukasiewicz@tlen.pl

Damian Szlachter, PhD

Editor-in-chief of the ISA (ABW) scientific journal "Terrorism – Studies, Analyses, Prevention". Member of the steering committee of the EU Protective Security Advisors group. National expert at the European Commission's Directorate-General for Migration and Home Affairs in the Policy Group on Public Spaces Protection. National auditor for quality control in civil aviation security (of the Civil Aviation Authority). Participant in the work of more than a dozen inter-ministerial teams and state administration working groups tasked with building resilience to terrorist and hybrid threats to strategic facilities for state security and critical infrastructure. Member of the team to investigate the challenges of engineering security of critical infrastructure buildings at the General Office of Construction Supervision. Author of nearly 40 scientific articles and co-author of several books and specialist reports on internal security.

Contact: d.szlachter@abw.gov.pl