Radosław Gross, MA
WSB University in Dąbrowa Górnicza
e-mail: radoslaw.gross@wsb.edu.pl
ORCID: 0000-0002-0915-4263

Rui Albuquerque, PhD
Lusófona University of Porto
e-mail: p2363@ulusofona.pt

DOI: 10.26410/SF_1/23/13

UNMANNED AERIAL VEHICLES AS A SOURCE OF THREATS TO CRITICAL INFRASTRUCTURE FACILITIES

Abstract

In accordance with the scope defined by the Polish legislation, the critical infrastructure in Poland consists of 11 systems, which are crucial for the security of the State and its citizens. These systems, because of the importance attached to them, must be subject to special, far-reaching protection. Critical infrastructure in each state plays a special role in ensuring continuity of operations of the state and its bodies. The efficiency of critical infrastructure is directly proportional to ensuring an adequate level and continuity in the distribution of services for which the state is responsible. The proper and safe functioning of the facilities that make up the critical infrastructure allows for the most efficient use by the state of the resources that should be mobilised in emergency situations that destabilise normal functioning of the state and its economy. Critical infrastructure is exposed to many types of attacks that aim to destabilise and disrupt proper functioning of the state. In terms of critical infrastructure protection, the state should take all measures to ensure full functionality, continuity of operations and integrity of critical infrastructure. It should be particularly proactive in preventing risks and threats and seek to reduce and neutralise the

impact thereof. Critical infrastructure should be restored immediately in the event of failures, attacks and other incidents that disrupt its proper functioning.
With the development of technology and engineering, a number of new sources of threats generated by modern equipment against critical infrastructure facilities have emerged. One increasingly common threat is from unmanned aerial vehicle platforms. Unmanned aerial vehicles (UAVs) are extremely versatile devices that can be used in a wide variety of ways and it is up to the pilot's skills, intentions and a chosen target to determine how the attack will be carried out and what threats it will induce. Given the seriousness with which the protection of critical infrastructure must be treated, it is important to note the scale of the risks associated with the use of UAVs. Each state should create both legal as well as actual opportunities through which the operator of critical infrastructure will be able to minimise or even eliminate the risk of unlawful use of unmanned aerial vehicles as tools to attack critical infrastructure.

Key words

critical infrastructure, unmanned aerial vehicles, drones, critical infrastructure protection, anti-drone systems

Methodology and methodological assumptions

The aim of this article is to present unmanned aerial vehicles as a source of threats to critical infrastructure.

The article defines critical infrastructure and its importance in the functioning of the state and society and provides a definition of unmanned aerial vehicles (UAVs). It also identifies the types of threats they may pose to critical infrastructure systems. The article divides risks into internal and external, the form in which they arise into unintentional and intentional, as well as forms and methods of risk mitigation.

The research problem identified by the author is the risks posed by the use of UAVs in the generation of threats that lie on the side of critical infrastructure. Theoretical and empirical methods, research techniques and tools were used to address the research problem identified above. The hypotheses of the article were formulated as follows:

- UAVs are highly technical devices which, due to their versatility and diversity of use, can be used to generate threats on the side of critical infrastructure as tools of attack,
- the pilot's knowledge and skills are both a risk mitigation factor and a tool for threat generation on the critical infrastructure side,
- all legally permissible activities should be undertaken to ensure the protection of critical infrastructure.

The conclusion critically addresses the solutions and tools available to Critical Infrastructure Operators to protect it from threats. The degree of independence and power they have to ensure effective protection against the threats posed by drones was considered insufficient. Directions and forms of change that contribute to the reduction or disqualification of risks are also indicated.

Introduction

Defining the concept of critical infrastructures is a complex task due to the variety of facilities and services that it is comprised of and their constant evolution, and thus the variety of threats that can cause disruption to such infrastructure[1]. Critical infrastructure is a term used to refer to the resources of a state that are important to the functioning of the state itself and of its economy and society. According to the legal definition contained in the legislation, critical infrastructure is considered to be 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 businesses[2]. According to the scope defined by the Polish legislator, the critical infrastructure in Poland consists of 11 systems, which are crucial for the security of the state and its citizens. Critical

1 J. Milewski, *Identification of Critical Infrastructure and its* Threats, „Scientific Journals of Akademia Obrony Narodowej"2016, No. 4 (105).

2 Art. 3(2) of the Act of 26 April 2007 on crisis management, consolidated text according to the Announcement of the Speaker of the Sejm of the Republic of Poland of 1 December 2022 on the announcement of the consolidated text of the Act on crisis management, Journal of Laws of 2023, item 122.

infrastructure includes the following systems:
- supply of energy, raw materials, fuels,
- communication,
- ICT networks,
- financial,
- provision of food,
- water supply,
- health protection,
- transport,
- rescue,
- ensuring continuity of public administration,
- (k) production, storage, warehousing and use of chemical and radioactive substances, including pipelines for hazardous substances[3].

Before the Critical Management Act came into force, individual issues were covered by various laws, most of which regulated the conduct of specialised services to counteract specific threats. However, there was no system for the protection of critical infrastructure, ensuring the direction and coordination of anti-crisis actions in the event of various threats, whether occurring throughout the state or in parts of it.[4]

Critical infrastructure is crucial to the existence of the State and, within it, of organised society. If there is a disruption in its functioning, the state and its institutions may lose all or part of their ability to perform their core administrative and service functions, as well as to exercise effective control over their entire territory[5]. Guaranteeing its proper functioning is one of the basic tasks of internal security[6]. The importance of critical infrastructure stems directly from the fact that its proper, uninterrupted operation is crucial to the provision of basic societal needs and services, both nationally and internationally. Moreover, an extremely important fact should be emphasised here, which shows that the protection and defence of individual elements of the critical infrastructure system does not belong solely to a matter of national interest.[7] In accordance with the provisions constituting the functioning of the European Community, and in line with the principle of shared responsibility, steps have been taken to define and introduce protective regulations concerning the European Union's critical infrastructure, recognising the important role it plays in the functioning of the Community security system.

Ensuring the security of critical infrastructure facilities

The complexity of this system and its sensitivity makes it vulnerable to a wide range of threats, both external and internal. These incidents may be caused either by forces of nature or as a consequence of human action, with the result

3 Ibidem.

4 A. Panasiuk, S. Sierański, *Protection of critical infrastructure facilities*, "State Control" 2017, No. 1.

5 K. Stec, *Selected Legal Tools for Critical Infrastructure Protection in Poland, National* Security, „Bezpieczestwo Narodowe" 2011, no. 19, III.

6 M. Modelski, *Identification and protection of critical infrastructure in Poland*, "Scientific Journals" 2018, No. 1-2.

7 W. Kawka, *Conditions for using non-lethal weapons of new generation as components of critical infrastructure system in the environment of hybrid threats, Problems of Technology and Armaments,* Wojskowy Instytut Techniczny Uzbrojenia, Journal 159 no. 1/2022.

that critical infrastructure can be destroyed, damaged, disrupted and thereby cause danger to life and property of the public[8]. Security depends to a large extent on public administration bodies, which perform many tasks in relation to crises and emergencies[9]. Nevertheless, in accordance with the crisis management act, critical infrastructure protection obligations are incumbent on the owners and parties acting as owners or holders under title other than ownership, of critical infrastructure facilities, equipment or systems. Whether or not a facility belongs to critical infrastructure is determined by detailed criteria listed in a classified annex to the National Programme for Critical Infrastructure Protection[10]. The decision to add a facility to the list of critical infrastructure shall be taken by the Director of the Governmental Centre for Security in cooperation with the relevant ministries, who shall inform the owner of the critical infrastructure of the fact that their facility has been added to the list. Owners, parties acting as owners and holders under title other than ownership, of critical infrastructure facilities or systems, the so-called Critical Infrastructure Operators, are obliged to protect it, in particular through preparation and implementation of critical infrastructure protection plans. These plans should include, inter alia: information on the critical infrastructure facility, description of threats and essential options for dealing with crises. The details and requirements of the aforementioned plans, including the rules for developing and discussing them, are set out in the Regulation of the Council of Ministers of 30 April 2010 on critical infrastructure protection plans[11].

The crux of critical infrastructure protection tasks is not only to ensure protection against threats, but also to act in such a way that time of any damage and disruptions to its functioning is as short as possible and the damage or disruptions can be easily remedied, without causing serious damage to citizens and the economy. In Poland, there exist a model of fragmented responsibility for protection of critical infrastructure[12]. Both the legislator and other decision makers place the responsibility for protecting critical infrastructure on its operator, on the assumption that they have the best knowledge of the facilities under their control. It is Critical Infrastructure Operators who, within their capacities, are in the best position to mitigate threats and reduce vulnerability, as well as the knowledge how to choose the most appropriate strategies to minimise the effects of threats. With these considerations in mind, they are obliged to:

8 A. Lasota-Jędrzejak, *Security of the State's Critical* Infrastructure, "Yearbook of Maritime Security" 2013, Year VII.

9 W. Bednarczyk, M. Kopczewski, *Tasks of Public Administration in the System of Critical Infrastructure Protection,* "Scientific and Methodical Review, Education for Security" 2017, Year X, Nymer 3/2017 (36).

10 *National Programme for the Protection of Critical Infrastructure for 2023*, file:///C:/Users/44737/Downloads/National-Program-Protection-of-CriticalInfrastructure-2023-text-uniform-2.pdf (access: 14.05.2023 r.).

11 Regulation of the Council of Ministers of 30 April 2010 on plans for the protection of critical infrastructure, Journal of Laws of 2010, No. 83, item 542.

12 M. Druszcz, *Use of unmanned aerial vehicles for the protection of critical infrastructure line installations*, "Police Review" 2018, No. 4 (132).

– preparation and implementation, in accordance with the risks anticipated, of critical infrastructure protection plans and maintaining own back-up systems providing security and sustaining the functioning of that infrastructure until it is fully restored,
– designate a person responsible for liaising with entities relevant for critical infrastructure protection,
– immediate forwarding to the Head of the Internal Security Agency information concerning threats connected with terrorist threats to critical infrastructure,
– cooperation in the development and implementation of the Programme[13].

The set of critical infrastructure protection activities means all activities aimed at ensuring the functionality, continuity of operations and integrity of critical infrastructure in order to prevent, mitigate and neutralise threats, risks or vulnerabilities, and to restore them rapidly in the event of failures, attacks or other events disrupting their proper functioning[14]. The critical infrastructure operator is therefore obliged to take all legal and factual measures to ensure the security of the facility.

Threats to critical infrastructure from unmanned aerial vehicles

With the development of technology and engineering, a number of new sources of threats generated by modern equipment against critical infrastructure have emerged. Innovative technologic solutions are, on the one hand, an advantage, but on the other hand they make modern states more vulnerable to the dangers that can hit their trouble spots[15]. The (almost unlimited) use of unmanned aerial vehicles in Polish airspace has recently become an increasing problem. These devices are beginning to be produced and used on a mass scale. Their price has become affordable for almost everyone and, as a result, they will increasingly appear in Polish airspace[16]. As such, it is a natural process that the threats from unmanned aerial vehicles and platforms exist. The threat in this case is the possibility of a pilot acting with an unmanned vehicle with the aim of carrying out an attack on humans or objects[17].

Unmanned aerial vehicles (UAVs) and unmanned aerial platforms (UAVs) are extremely versatile devices that can be used in a wide variety of ways and it

13 As set forth in Resolution no. 210/2015 of the Council of Ministers of 2 November 2015 on the adoption of the National Programme for the Protection of Critical Infrastructure, with consideration of Resolution No. 116/2020 of the Council of Ministers of 13 August 2020 amending the resolution on the adoption of the National Programme for the Protection of Critical Infrastructure and Resolution No. 38/2023 of 21 March 2023 amending the resolution on the adoption of the National Programme for the Protection of Critical Infrastructure.

14 Article 3(3) of the Act of 26 April 2007 on crisis management, consolidated text according to the Announcement of the Speaker of the Sejm (one of the chambers of the Parliament) of the Republic of Poland of 1 December 2022 on the announcement of the consolidated text of the Act on crisis management, Journal of Laws of 2023, item 122.

15 I. Bunsh, J. Świątkowska, *New trends in the area of critical infrastructure protection – a European perspective*, "Scientific Work of Wałbrzyska Wyższa Szkoła Zarządzania i Przedsiębiorczości" 2013, T. 25 (5).

16 J. Kasperkiewicz, *Unmanned aerial vehicles (drones) and the latest draft legal regulations on their use*, "University of Warsaw Law Review" 2015, Year XIV, No. 1/2015.

17 J. Łukasiewicz, *Offshore wind farms as potential targets for attack using unmanned aerial vehicles*, "Government Security Centre Quarterly Bulletin" 2021, Number 32.

is up to the pilot's intentions and chosen target to determine how the attack will be carried out. A drone can carry a hazardous substance (e.g., viruses or bacteria) over larger concentrations of people (e.g., at mass events or demonstrations). Another example would be the appearance of a drone with a small explosive charge, such as over an airport or a large oil tank at a fuel depot. Left unnoticed, a small unmanned flying object can paralyse airport traffic or endanger the health and lives of people by placing a payload in an oil port, which is connected with huge financial losses[18]. Also, the equipment of drones is significant from the point of view of the risks that UAVs can generate. Unmanned aerial vehicles are now identified with machines equipped with the latest electronic and navigation systems[19].

A key feature of UAVs is that they are devices that carry out their missions without a pilot on board. This feature results in the pilot controlling the device from the ground being inclined to carry out operations that are riskier and therefore entail greater risks than aircraft with a human factor on board. Given the seriousness with which critical infrastructure protection should be treated, risks associated with the use of unmanned aerial vehicles should be taken into account by critical infrastructure operators as very likely to occur.

It is important to be aware that the airspace around critical infrastructure is the least secure and that flights with the use of unmanned aerial vehicles can practically be performed with impunity[20]. Every flight of an unmanned aircraft over or near critical infrastructure facilities entails a specific risk. The level of risk also depends on the form of the mission, taking into account the premise of whether the UAV is flown manually or autonomously. The most straightforward and basic in implementation and yet requiring the highest level of manual skills is the manual control system for unmanned aircraft. The manual system requires the pilot to use the control apparatus and a certain level of manual skill and knowledge of aerodynamic principles, as well as an understanding of the environment in which the flight operation is performed. The second type of control system is semi-automatic, where the pilot programmes the UAV as to the flight path and its parameter. Semi-automated systems are programmed so that the flight follows a predetermined route and the unmanned aircraft reacts to basic external stimuli such as obstacles. Fully autonomous systems are the most advanced in its operation. In this case, artificial intelligence algorithms are used to ensure that the UAV is able to make decisions autonomously as well as to carry out missions without a pilot. Threats of UAVs operating autonomously and programmed to fly around designated GPS points are much greater

18 G. Pietrek, *Threats to critical infrastructure. The case of unmanned aerial vehicles*, "Journal of Modern Science" 2022, Volume 2/49/2022.

19 J. Chojnacki, D. Pasek, *History of the use of unmanned aerial vehicles*, "International Security Yearbook" 2017, vol. 11, no. 1.

20 G. Pietrek, M. Pietrek, *Unmanned aerial vehicles as a threat to critical infrastructure*, "Scientific Journals of Fire Service School" 2022, no. 83.

due to UAVs ability to operate without RC apparatus and the lack of detection of such communications.

Considering the effect and purpose for which it can be used, it can be concluded that UAV can be used as a tool for non-kinetic and kinetic attacks on critical infrastructure objects. Based on the author's own experience, several basic groups of threats to critical infrastructure from UAVs can be distinguished. These are: industrial or military espionage, terrorism, causing communications disruption, kinetic attacks or, finally, invasion of privacy. In terms of the threat in the form of industrial or military espionage, UAVs equipped with specific recording devices such as various types of video, thermal or multispectral cameras and sound recording devices are able to collect sensitive information related to the construction, equipment and operation of a critical infrastructure facility. They can also be used to identify technologies used in critical infrastructure facilities and analyse security vulnerabilities. In the case of destructive attacks, UAVs with the appropriate equipment capable of carrying various types of explosives, chemicals or cyber-attack triggers are able to carry out an operation aimed at destroying a facility or disabling its key systems. Interference with communication systems particularly affects telecommunications networks, GPS and similar systems or radars. Special unmanned aircraft equipment such as signal scanners or jammers may interfere with data transmission or lead to communication interruptions and generate erroneous navigation system readings, which can have far-reaching consequences for critical infrastructure facilities, in particular aviation or transport facilities and telecommunications or energy networks. In the case of direct attacks, due to its own weight and the kinetic force generated, an unmanned aerial vehicle may pose a risk causing accidents and damage to critical infrastructure due to the significant impact force generated. In terms of privacy issues, due to the increasingly sophisticated recording devices they may be equipped with, unmanned aerial vehicles are capable of recording sensitive data in the form of video or audio for further use in an unlawful manner.

A successful attack on critical infrastructure has many consequences with effects on different levels: from economic, social and political to ecological and finally political. With this in mind, we note what a broad spectrum UAVs represent in terms of threat generation to critical infrastructure. Example attack targets:

- observation/identification of the equipment of which the physical protection system is constructed,
- observation of the activities of physical security personnel, gaining information on procedures,
- identification of persons working in the protected facility,
- gaining information on the technology used at the protected facility,
- bugging the communication of physical security personnel or staff working in the facility,
- physical damage to equipment used in the facility's process,

– significant damage to equipment, installations, paralysing the operation of the facility,
– causing environmental contamination in or around the facility[21].

Possible accumulation of threats from the unlawful use of UAVs against critical infrastructure facilities is also worth noting. Links between systems and elements of critical infrastructure their failure or temporary disruption may lead to malfunction of other systems[22]. Accumulation of threats may occur, for example, in the case of an attack on an energy network, the proper functioning of which is essential to ensure the continuity of operation of other critical infrastructure facilities. The aforementioned circumstances also illustrate how a single failure of the system infrastructure can have a domino effect – the emergence of many other security threats occurring at different locations[23].

All threats on the side of critical infrastructure can be divided according to the form in which they arise. Here we distinguish between unintentional and intentional actions. An unintentional event with the use of UAVs is considered to be one that occurs for random reasons, e.g. as a result of weather conditions (high winds) or reasons attributable to the pilot and his inadequate skills on the part of the pilot or for reasons attributable to the device when an accidental, unplanned but dangerous attack on a critical infrastructure site occurs. Such a situation will be encountered, for example, when a pilot inadvertently violates a prohibited zone or, as a result of an equipment malfunction, performs a flight operation that threatens the infrastructure. Intended operations, on the other hand, are any intentional human action characterised by a terrorist nature or any other premeditated action, e.g. of an economic-political nature. While unintentional actions do not aim to intentionally cause damage, intentional actions aim to cause the widest possible damage to a critical infrastructure facility or the highest possible benefit to the initiator of the attack. However, it is worth noting that both threats caused by unintentional causes and those caused intentionally in the same way have a negative impact on the functioning of the entire critical infrastructure system or cause adverse changes in its environment, both internal and external.

Ways to minimise or eliminate the risks associated with the use of unmanned aerial vehicles against critical infrastructure facilities

In order to prevent threats to critical infrastructure caused by UAVs, it is necessary to take appropriate measures to prevent or minimise the risks of attack. What is needed is both the introduction of systemic solutions by defining specific legal solutions minimising the risk of attacks, as well as appropriate technical

21 Ibidem.

22 J. Łukasiewicz, M. Piekarski, M. Kluczyński, *Security of critical infrastructure in the face of threats from unmanned platforms*, Polish National Security Association, "PTBN Report" 2021, volume II.

23 S. Kolano, *Identifying threats to the state's critical infrastructure*, „Public Security" 2018, notebook 12/2018.

actions aimed at monitoring, detection and neutralisation of UAVs.

Any risks of an unintended nature can be minimised or disregarded altogether, both through the introduction of relevant legislation sanctioning unmanned aircraft operations and through educational measures addressed to the pilots performing the flights. It is worth pointing out two main issues in terms of legal solutions favouring risk mitigation in relation to facilities classified as critical infrastructure. Directly influencing the reduction of risk in this respect is, firstly, the system of acquiring authorisations by pilots of unmanned aerial vehicles, secondly, the introduction of geographical zones in Polish airspace and, finally, the procedures and requirements imposed on operators in connection with their operation and its scope. Ultimately, it is important to implement appropriate training with adapted topics and scope, in such a way as to reduce the risk of a dangerous situation arising, thereby increasing the safety of the public[24].

The legal requirements to which UAV pilots are subject mainly depend on the purpose of the flight, which may be sport – leisure or other than sport – leisure[25]. National regulations[26] generally divide UAV operations by purpose (sport/leisure, other), type (with or without UAV visibility) and MTOM weight categories[27]. Attention should be paid to the fact that in the regulations sanctioning the use of unmanned aircraft as well as the requirements for pilots, Poland has explicitly introduced regulations developed at European Commission level. Implementing Regulation 2019/947 of the European Commission, which has been implemented into the Polish legal system, establishes specific rules for the operation of unmanned aircraft systems and for personnel, including pilots of unmanned aerial vehicles and organisations involved in operations with the use of them[28]. In addition, European Commission Delegated Regulation 2019/945 establishing requirements for the design and manufacture of unmanned aerial vehicles intended to be operated in accordance with the principles and conditions set out in the previously mentioned Regulation and additional elements for remote identification has been implemented. It also defines the types of UAVs whose design,

24 A. Karolewski, M. Rejman-Karolewska, *Protection of critical infrastructure*, "Scientific and Methodical Review, Education for Security" 2015, Year VII, Number 2/2015 (27).

25 M. Feltynowski, *Use of unmanned aerial platforms in public safety operations*, Warszawa 2019.

26 Announcement of the Minister of Infrastructure and Construction of 27 October 2016 on the announcement of the consolidated text of the Regulation of the Minister of Transport, Construction and Maritime Economy on the exclusion of the application of some provisions of the Aviation Law Act to some types of aerial vehicles and the determination of conditions and requirements for the use of these vehicles, Annex 6 and 6a (Journal of Laws item 1993) and the Regulation of the Minister of Infrastructure of 20 December 2018 amending the Regulation on the exclusion of the application of some provisions of the Aviation Law to some types of aerial vehicles and the determination of conditions and requirements for the use of such vehicles (Journal of Laws of 2019, item 94).

27 W. Wyszywacz, *Safety of Air Operations in the Aspeck of Training and Work*, [in:] M. Feltynowski, *Use of Unmanned Aerial Platforms in Public Safety Operations*, Warszawa 2019.

28 Commission Implementing Regulation (EU) No. 2019/947 of 24 May 2019 on rules and procedures for the operation of unmanned aerial vehicles, Journal of Laws L152 of 11.06.2019.

manufacture and maintenance are subject to certification[29].

Depending on the level of risk of the operation, flights with the use of unmanned aerial vehicles can take place in one of three categories, for which specific requirements have been defined that pilots should meet. Three categories can be identified, each entailing a different level of risk:

- open category- for low-risk flying in VLOS (Visual Line of Sight) conditions,
- special category – for medium risk, VLOS and BVLOS (Beyond Visual Line of Sight) flights which do not fall into the open category,
- certified category – for high-risk flights with certified design, manufacture and maintenance of airworthiness of UAVs weighing more than 25 kg.

A common feature of the requirements for pilots of unmanned aerial vehicles, regardless of the aforementioned purposes of their flights, is the acquisition of a specific level of knowledge as well as an awareness of the risks involved in flight operations. The first step towards gaining an unmanned aircraft licence in the open category is to carry out the procedure of applying (logging in) as an operator to the Civil Aviation Authority[30]. Operators have the possibility to apply and log in in any of the Community states. Operators of unmanned aerial vehicle systems shall register in accordance with their place of residence or, in the case of legal persons, in the country where they have their principal place of business. Once you have registered as an operator, you must submit your pilot profile for confirmation. Via the pilot's profile, it is possible to take the training and online examination for basic subcategories for the open category – A1/A3, followed by the theoretical training part for open subcategory A2. The A2 category test itself is conducted by an external, Civil Aviation Authority-designated body. A designated entity is a qualified entity under the so-called Base Regulation[31].

In the case of the special category, flights are operated on the basis of standard scenarios or an individual permit obtained by the operator from the President of the Civil Aviation Authority or on the basis of a previously obtained LUC certificate. National flight standard scenarios have been introduced by the President of the Civil Aviation

29 Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aerial systems and operators of unmanned aerial systems from third countries, Journal of Law L152 of 11.06.2019.

30 https://drony.ulc.gov.pl/ (accessed 17.05.2023).

31 Regulation (EU) of the European Parliament and of the Council of 4 July 2018, 2018/1139 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency. Aviation Safety and amending Regulations of the European Parliament and of the Council (EC) No. 2111/2005, (EC) No. 1008/2008, (EU) No. 996/2010, (EU) No. 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council and repealing Regulations (EC) No. 552/2004 and (EC) No. 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No. 3922/91, Official Journal of the European Union L212/1 of 22.08.2018.

Authority by way of guidelines[32]. In this situation, a flight may be performed after the operator has submitted a declaration to the Civil Aviation Authority that the flight will be performed within a specific scenario. Once the declaration has been submitted, the operator receives confirmation that the submitted documentation is correct and complete, thus gaining the right to perform the flight operation within the limitations imposed by the scenario. A specific situation occurs when the flight operation being performed both falls outside the open category and goes beyond the standard scenarios. In this case, approval for the operation must be obtained from the President of the Civil Aviation Authority before it can be carried out. In order to obtain it, the operator is required to carry out an individual risk assessment of its planned flight operation. In practice, there are two alternative forms of assessing the risks posed by the operation to be carried out: carrying out a risk assessment of the planned operation according to the SORA methodology[33] or make a Pre-Defined Risk Assessment

32 National Standard Scenario NSTS-01 – Guidance Note No. 15 on National Standard Scenario NSTS-01 for visual line of sight (VLOS) or first-person view (VPV) operations using an unmanned aerial vehicle with a take-off mass of less than 4 kg, Official Journal of the Civil Aviation Office, 30 December 2020, item 69,

National Standard Scenario NSTS-02 – Guidance Note No. 16, on National Standard Scenario NSTS-02 for visual line of sight (VLOS) operations using unmanned aerial vehicles in the multi-rotor (MR) category with a take-off mass of less than 25kg, Official Journal of the Civil Aviation Office, 30 December 2020, item 70

National Standard Scenario NSTS-03 – Guidance Note No. 17, on National Standard Scenario NSTS-03 for visual line of sight (VLOS) operations using unmanned aerial vehicle in fixed-wing category (A) with a take-off mass of less than 25 kg, Official Journal of the Civil Aviation Office, 30 December 2020, item 71

National Standard Scenario NSTS-04 – Guidance Note No. 18, on National Standard Scenario NSTS-04 for visual line of sight (VLOS) operations using unmanned aerial vehicle in the helicopter (H) category with a take-off mass of less than 25 kg, Official Journal of the Civil Aviation Authority, 30 December 2020, item 72

National Standard Scenario NSTS-05 – Guidance Note No. 19, on National Standard Scenario NSTS-05 for Beyond Visual Line of Sight (BVLOS) operations using unmanned aerial vehicle with a take-off mass of less than 4kg, within 2km of the pilot of the unmanned aircraft, Official Journal of the Civil Aviation Office, 30 December 2020, item 73

National Standard Scenario NSTS-06 – Guidance Note No. 20, on National Standard Scenario NSTS-06 for beyond visual line of sight (BVLOS) operations using unmanned aircraft in the multi-rotor (MR) category with a take-off mass of less than 25 kg, within 2km of the pilot of the unmanned aerial vehicle, Official Journal of the Civil Aviation Office, 30 December 2020, item 74

National Standard Scenario NSTS-07 – Guidance Note No. 21, on National Standard Scenario NSTS-07 for Beyond Visual Line of Sight (BVLOS) operations using unmanned aircraft in fixed-wing category (A) with a take-off mass of less than 25 kg, within 2km of the pilot of the unmanned aerial vehicle, Official Journal of the Civil Aviation Office, 30 December 2020, item 75

National Standard Scenario NSTS-08 – Guidance Note No. 22, on National Standard Scenario NSTS-08 for Beyond Visual Line of Sight (BVLOS) operations using unmanned aerial vehicle in the helicopter category (H) with a take-off mass of less than 25 kg, within 2km of the pilot of the unmanned aerial vehicle, Official Journal of the Civil Aviation Office, 30 December 2020, item 76

National Standard Scenario NSTS-09 – Guidance Note No. 21, on National Standard Scenario NSTS-07 for Beyond Visual Line of Sight (BVLOS) operations using unmanned aerial vehicles with a take-off mass of less than 25kg, performed by operators of unmanned aerial vehicle systems holding a national permit to fly (BVOLS), Official Journal of the Civil Aviation Office, 30 December 2020, item 77

33 SORA – Specific Operation Risk Assessment, is a methodology for creating a risk analysis by which an operator flying an unmanned aerial vehicle verifies the aerial operation for safe performance. Published in AMC1 to Commission Implementing Regulation (EU) No 2019/947 of 24 May 2019 on rules and procedures for the operation of unmanned aerial vehicles. Journal of Laws L152 of 11.06.2019.

(PDRA)[34]. The third form of special category flying is to first obtain a LUC certificate guaranteeing that the holder of the certificate ensures a high level of safety in performing flight operations. The LUC certificate is a light unmanned aircraft system operator certificate issued after the operator has met certain flight safety assurance requirements[35].

The category with the highest degree of risk is the certified category. Aerial operation by unmanned aerial vehicle qualifies as certified category if any of the following conditions are fulfilled: the flight is performed over congregations of persons, the operation involves transport of persons, or the operation involves the transport of hazardous materials which, in the event of an accident, could pose a risk to third parties. It covers VLOS and BVLOS flights whenever they are performed with unmanned aircraft requiring certification in accordance with Delegated Regulation (EU) 2019/945. Flights in this category are comparable, in terms of the risk they entail to bystanders, to the level of risk involved in flying manned aerial vehicles.

Regardless of the category in which the flight is performed, the pilot has knowledge of the rules of flights, the risks involved in flight operation, as well as the shape of the Polish airspace and the restrictions and prohibitions on operating unmanned aerial vehicles. A specific and effective way of mitigating risks to objects that are elements of critical infrastructure is the introduction of geographical zones in Polish airspace. The introduction of the geographic zones is an offshoot of the obligations imposed on member states by Commission Implementing Regulation (EU) 2019/947. By geographical zone, as defined, we mean that part of the airspace designated by the competent authority which facilitates, limits or excludes operations using unmanned aircraft in order to eliminate risks to safety, privacy, data protection, security or the environment, arising from operations using unmanned aerial vehicle systems. In Polish airspace, geographical zones have been created by the Polish Air Navigation Services Agency in connection with the delegation to it, by the President of the Civil Aviation Office, of the authority to designate them[36]. In accordance with the Guidelines of the President of the ULC, five types of zones have been designated[37]. From our point of view the most important for the

34 The PDRA is a simplified form of operator risk analysis proposed by the European Union Aviation Safety Agency (EASA). Where the planned operation falls within the published PDRA, the instructions contained therein can be followed while waiving the preparation of a full risk analysis. https://www.easa.europa.eu/en/document-library/easy-access-rules/easy-access-rules-unmanned-aircraft-systems-regulations-eu (accessed 17.05.2023).

35 The LUC Certificate is issued upon fulfilment of the conditions set out in paragraph 1, Part C, UAS.LUC.050, to Commission Implementing Regulation (EU) No 2019/947 of 24 May 2019 on rules and procedures for the operation of unmanned aerial vehicles. Journal of Laws L152 of 11.06.2019.

36 Guideline No. 24, President of the Civil Aviation Authority, Official Journal of the Civil Aviation Authority, on designation of geographic zones for unmanned aerial vehicle systems, 30 December 2020, pos. 78.

37 In accordance with § 3.1. of Guidelines 24, Polish airspace is divided into the following zones: DRA-P -prohibited zone, DRA-R -restricted zone for unmanned aerialvehicle systems, DRA-T – restricted zone for unmanned aircraft systems, in which the Agency indicates technical requirements, DRA-U – geographical zone for unmanned systems unmanned aircraft aircraft, in which operations of unmanned systems aircraft aircraft may take place take place only with the support of specific, verified services provided in this zone, DRA-I – information zone.

reduction or elimination of risk on the part of the critical infrastructure facilities covered by the territorial scope of the designated zone is the designation of DRA-P – prohibited zone, in which operations using unmanned aerial vehicle systems may not be carried out, and DRA-R – restricted zone for unmanned aerial vehicle systems, in which operations using unmanned aerial device systems may be carried out with the permission under conditions specified by the Polish Air Navigation Services Agency or the authorised entity, at the request of which the geographical zone was designated. Precise coordinates of the zones' locations are available on the Polish Air Navigation Services Agency website[38] and in the DroneRadar mobile application[39].

Pursuant to § 5(1)(2) of Guideline No. 24 of the President of the Civil Aviation Authority, due to the needs of critical infrastructure protection, the entities entitled to submit an application for designation of a zone are the Commander-in-Chief of the Police, the Chief of the State Fire Service and the Director of the Government Security Centre. When designating a zone, its vertical and horizontal boundaries and activity time directives and, in the case of DRA-R zones, the flight conditions are defined. In such a situation, the designation of zones can be regarded as a tool that, through anticipatory action, prevents risks to the critical infrastructure facilities in the zone resulting from flights of unmanned aerial vehicles.

It is noteworthy that only a small group of facilities classified as critical infrastructure are covered by the territorial scope of designated zones. This does not mean that other facilities do not remain under the special attention of those responsible for ensuring security. In the guidelines of the President of the Civil Aviation Office, which are a specific form of legal norms, special attention is directed at certain groups of facilities classified as critical infrastructure. In accordance with the provisions of Appendix No. 1 to Guideline No. 7 of the President of the Civil Aviation Office of 9 June 2021, both during open category operations (chapter 2, point 2.2) and special category operations (chapter 2, point 3.3), flights over: seaports, power stations, water intakes and sewage treatment plants as well as military units and training grounds may only be performed with the consent or for the purposes of the facility manager[40]. In addition, in accordance with Chapter 2, Section 2.3 (for the general category) and Section 3.4 (for the special category), a duty of extreme caution has been introduced for flight operations using unmanned aircraft systems over: fuel pipelines, power and telecommunications lines, dams, sluices and other open-air facilities, the destruction or damage of which may endanger human life or health, the environment or cause serious damage to property.

38 Map of geographical zones Polish Air Navigation Services Agency: https://airspace.pansa.pl/map (accessed 17.05.2023).

39 Map of geographical zones of the DroneRadar app: https://droneradar.eu/ (accessed 17.05.2023).

40 Guideline No. 7, President of the Civil Aviation Authority, on ways to perform operations with using systems unmanned aircraft in connection with entry into force provisions of Commission Regulation (EU) No. 2019/947 of on 24 May 2019 on regulations and procedures for operation of unmanned aircrafts, 9 June 2021, Item 35.

The measures described above, which can be considered to minimise or exclude incidents threatening critical infrastructure and which are unintentional in nature, are objectively sufficient for the purpose for which they were introduced. Obviously, legislation as well as the solutions introduced by those responsible for security will not fully eliminate the possibility of danger. Nevertheless, they contribute to minimising it. In terms of unintentional hazards, an important factor is also the level of awareness of the pilot himself, but here only full professionalism in the approach to the execution of the flight operation will result in the disqualification of threats.

The situation is different in the case of threats of an intentional nature, where it is the action of the pilot, the user of the unmanned aerial vehicle, that is intended towards causing as much damage or gaining as much benefit as possible from an attack on a critical infrastructure facility. In such a situation, no legal regulations and/or standards can prevent the threat, and only measures taken against such attacks in both passive and active forms contribute to minimising losses or lead to the elimination of risk. The recommendations come down to the main postulate that it is necessary to introduce effective protection systems, including anti-drone, very widely. Such systems are already developed or are in the final stages of certification. The systems are diverse and can be freely configured depending on the needs and financial resources available to protect IK.

An important element in the CIP regime is the statutory delegation to destroy or immobilise an unmanned aerial device when it poses a threat[41]. Pursuant to the wording of Article 126a of the Aviation Act, an unmanned aerial vehicle may be destroyed, rendered inoperative or its flight may be taken over in cases where, inter alia: it poses a threat to protected premises, facilities or areas (Article 126a, point 1, paragraph 1 b) and creates a reasonable suspicion that it may be used as a means of a terrorist attack (Article 126a, point 1, paragraph 1 d). In such cases, authorised officers of the Police, Border Guard, State Protection Service, Internal Security Agency, Intelligence Agency, Central Anti-Corruption Bureau shall destroy or immobilise the unmanned aircraft or take control over its flight, the Military Counterintelligence Service, the Military Intelligence Service, the Customs-Sanitary Service and the Prison Service, the Marshal Guard, soldiers of the Military Gendarmerie and the Armed Forces of the Republic of Poland and employees of specialised armed security formations.

The above solutions of a legal nature sanctioning the performance of aerial operations using unmanned aircraft are primary solutions that anticipate the occurrence of a threat on the part of critical infrastructure. Respecting the rules is one of the most significant elements depressing the functioning of the UAV market. The effectiveness of educational and sanctioning measures directly

41 Entitlement introduced by Article 126a, Act of 3 July 2002, Aviation Law, consolidated text introduced by the Announcement of the Speaker of the Sejm of the Republic of Poland of 28 April 2022, Journal of Laws of the Republic of Poland, Item 1235, 10.06.2022.

affects both the safety of flight operations and provides a tool to reduce or eliminate risks to critical infrastructure facilities. In addition, a way of mitigating the risk is, as shown above, a whole system of certification and verification of operators/pilots imposing on them a series of requirements that they must meet. The failure of the pilot and the operator of the unmanned aerial vehicle to comply with the above conditions will be important in assessing the degree of fault in the event that they cause damage, and thus their liability, both civil and criminal[42].

One of the most important aspects of combating or counteracting the effects of premeditated intentional action, and therefore the use of UAVs against critical infrastructure facilities, is the ability to detect and identify these devices early. The most commonly used methods for detecting unmanned aerial devices include:

- radar methods,
- methods to detect communication between a flying unmanned platform and a ground station,
- methods for detecting the acoustic signal emitted by the rotating parts of a flying unmanned platform,
- methods based on both visible and infrared image analysis[43].

Each of the above methods is pre-emptive and aims to identify an object in advance, as well as to predict a possible threat that the flight may pose to critical infrastructure objects. The more precisely a threat is identified, the easier it is to select from a catalogue of possible responses in such a way as to be most effective and to reduce the risk and possible consequences of an attack on critical infrastructure facilities as much as possible. An important performance characteristic of devices and systems that detect and identify threats on the side of critical infrastructure that entail the use of unmanned aerial vehicles is their speed and efficiency. This efficiency translates directly into response times for the services responsible for protecting the areas concerned, such as airports, railway stations or public facilities. Note that UAVs are not subject to the typical constraints found in road traffic, so they can traverse space directly along a straight line to their destination[44].

An analysis of the available electronic systems for protection against BSP shows two main design trends, the first being portable systems (carried by the operator or mounted on the vehicle) and the second being stationary systems. Both solutions have their advantages, in the case of portable systems the light weight and significant maneuverability of fire are pointed out, in the case of stationary systems – the long range and efficiency of neutralisation[45].

In practice, we can distinguish two ways of countering attacks from UAVs.

42 K. Wasilewski, *The Liability of the UAV Operator for the Preformed Flight*, [in:] M. Feltynowski, *Use of unmanned aerial platforms in public safety*, Warszawa 2019.

43 J. Łukasiewicz, *Unmanned aerial vehicles as a source of threats to the infrastructure of the supply of electricity to countries and proposed methods of protecting this infrastructure, Terrorism – studies, analyses, prevention*, „Terroryzm – studia, analizy, prewencja" 2022, No. 1 (1).

44 G. Pietrek, *Critical infrastructure security management, Anti-drone systems*, "Defence Knowledge" 2022, Vol. 280.

45 K. Górski, S. Szymański, I. Mielczarek, J. Grzesiak, *Electronic systems for protection against BSP*, "Electrotechnical Review" 2022, R. 98, No. 9/2022.

These are non-kinetic and kinetic methods. It can be said that the essence of countering unmanned aircraft systems is to provide protection against their use and its effects or to minimise the effects of their use. The non-kinetic way is to act on the UAV with various factors to neutralise it, while the kinetic way is to act by physical force. The most effective devices are those that are a hybrid of solutions, i.e., capable of both kinetic and non-kinetic impact.

The most common ways of neutralising UAVs include:

- interference with or jamming of the satellite navigation system,
- interference with the communication signal between the base station and the UAV,
- damage to electronic components by means of an electromagnetic pulse emitter,
- mechanical damage to or interception of a flying UAV,
- damage to the BSP using laser light by lighting it.

One of the non-kinetic ways to combat unmanned aerial systems is interference. In the literature we can distinguish between two basic techniques (ways) of intentional interference with radio-electronic devices, including those implemented on board of unmanned aerial vehicles. The most common term used to refer to interference is 'jamming'. It can be understood as the emission of electromagnetic waves towards the receiver of a signal (e.g. navigation) in order to interrupt its availability. Another deliberate means of intentional interference is 'spoofing' (signal falsification and impersonation). Spoofing is a type of electronic attack that works by emitting false navigation signals (e.g., GSP) that mimic real signals reaching the user from the system's satellites. Its purpose is to provide the user with incorrect positioning, velocity and timing information necessary to guide the aircraft[46]. Despite the fact that devices of this kind are effective, the possibility of using them to protect critical infrastructure from an attack using an unmanned aerial vehicle is purely illusory. Depending on their design, jammers and spoofers are either apparatus as defined in the Electromagnetic Compatibility Act[47] or radio equipment as defined in the Telecommunications Act[48]. One of the requirements for radio apparatus and equipment is that it is designed in such a way that it does not cause harmful interference or electromagnetic disturbance in its operating environment, which prevents other radio equipment using radio frequencies from working as intended. Taking these considerations into account, and the fact that the main function of jammers and spoofers is to prevent the effective use of radio frequencies by generating harmful interference or unacceptable electromagnetic disturbances in a particular electromagnetic environment, it is not possible to meet the statutory compliance requirements. Such equipment will therefore not receive a positive conformity assessment, which

46 R. Bielawski, *Safety of Unmanned Aerial Systems in a Disturbance Environment*, "De Securitate et Defensione, On Security and Defence" 2019, no. 2 (5).

47 Art. 6 item 1 of the Act of 13 April 2007 on electromagnetic compatibility, Journal of Laws of 2019, item 2388, as amended.

48 Article 2 para. 45 of the Act of 16 July 2004. Telecommunications Law, Journal of Laws 2019, item 2460, as amended.

implies that it cannot be legally marketed and used in the civilian critical infrastructure environment, both within the European Union and in Poland. These devices can therefore be used only in a military environment.

The second of the non-kinetic ways is to damage the electronic components of the UAV with an electromagnetic pulse emitter. The idea of using electromagnetic waves to interfere with electrical equipment is not new. As a result of its use, there will be no damage, no fire, no dead, no injured and still the effects will prove appalling. The emitted wave propagates through the surrounding space and reaches all kinds of electrical equipment, causing damage or destruction[49]. Devices of this type also have a high degree of efficiency. Their use, however, comes with certain limitations. Firstly, they are useless when the operation of a critical infrastructure facility directly depends on electricity and includes any electrical and electronic equipment. Secondly, this method cannot be used in case of an unmanned aircraft falling from a high altitude, where the impact force thus generated causes damage to the facility.

A form of kinetic neutralisation of an unmanned aerial vehicle that poses a threat to critical infrastructure is to damage or physically capture it. A direct action is a physical grounding, such as being caught in a net via another specialised drone or a net being fired by a ground-based cannon-launcher. Its biggest advantages are related to its speed and low operating cost. Among the risks are those associated with the drone falling to the ground uncontrollably or the explosion of the load it carries, with particularly negative consequences for critical infrastructure facilities[50]. Due to the need to deliver the interceptor element to the vicinity of the facility to be intercepted, the range of such systems is usually much shorter than that of jamming systems[51].

The last form of neutralisation of UAVs mentioned above is to use laser light and make it ignite. The light emitted by the laser illuminates the flared object, causing an increase in temperature and ultimately igniting its plating[52]. The very idea of using laser light is to act on its sensitive point by an unmanned aerial vehicle, the destruction of which (ignition, melting, etc.) will damage or destroy the entire facility. Such a sensitive component could be an optoelectronic system, a control system or a sheathing laminate. The advantage of this type of defensive action is its precision due to the directional action of the laser beam. The danger, on the other hand, comes from the generation of fire as a high damage factor.

49 T. Szubrycht, T. Szyma, *Electromagnetic weapons as a new means of warfare in the information age*, "Scientific Journals of Akademia Marynarki Wojennej" 2005, Year XLVI no. 3 (162).

50 S. Cheba, P. Kutyła, A. Mroczkowska, M. Olszewska, A. Szczukocki, P. Szkudlarek, J. Wierzbicka, *Delivering U-Space in order to boost Poland's competitivness, in Jarecki S.A., Modern infrastructure as a tool to build the strength and competitiveness of the Republic, collective work*, Report of the Students of the National School of Public Administration, 2020.

51 G. Leśnia, P. Płatek, Ł. Szmit, M. Czyżewska, M. Grązka, J. Michałowski, *Analysis of man-portable systems intercepting miniature unmanned aerial vehicles, Problems of Armament Technology*, "Journal" 2017, no. 2/2017.

52 R. Bielawski, *Safety of Unmanned Aerial Systems in a Disturbance Environment*, "De Securitate et Defensione, On Security and Defence" 2019, no. 2 (5).

Summary

Critical infrastructure plays a key role in ensuring the proper functioning of the state as well as having a significant impact on the level of security perceived by citizens. These considerations mean that its protection should be one of the priorities, as by protecting it we are able to ensure its proper functioning or rapid restoration in the event of damage. All types of critical infrastructure threats, whether natural or terrorist in origin, are becoming increasingly important due to the existence of increasingly interdependent systems. This interdependence directly generates increased vulnerability. In today's world, it is extremely important to correctly define threats, observe their evolution and also constantly analyse their impact. The knowledge gained in this way will, due to the changing nature of the risks, allow for the modification of the protective measures taken to date as well as the development of new preventive interactions. The economic factor is also not insignificant in terms of the quality and level of critical infrastructure security. Adequate and effective threat identification and subsequent protective action undoubtedly generate the expenditure of considerable financial resources. However, these measures are disproportionate to the expenditure that would have been incurred to restore critical infrastructure facilities.

One of the factors determining the effectiveness of protection against attacks is the response time to the threat. It should be noted that the primary objective of protection is to ensure the continuous operation of systems that constitute critical infrastructure. The development of specific patterns of behaviour as well as the prior definition of the methods to be used for protection contributes to ensuring its effectiveness.

As outlined in the article, developments in technology and techniques are contributing both to the evolution of the threats themselves and to an increase in the number of their types. Unmanned aerial vehicles, due to their popularity and permanent presence as commonly used equipment, are a significant factor in the risks generated on the part of critical infrastructure. Due to their functionalities and increasing excellence, they are growing in importance as tools used to attack protected facilities.

The article categorises events treated as an attack on critical infrastructure as unintentional and intentional. A list of risk prevention tools is also presented, and it should be stressed that, whatever their form, they are the same source of risk. Pilot training processes and imposed flight procedures as well as the shape of the country's airspace were identified as forms of counteracting unintentional attacks. Assessing the solutions introduced by the legal standards system, it can be said that they try to take into account the demands for reducing risks and hazards. The aforementioned level of awareness and responsibility of the pilot as well as the extent of the knowledge implemented will certainly not entirely eliminate the possibility of unintentional attacks, but it will certainly significantly reduce the level of threats to critical infrastructure facilities. Critically, it should be noted that, in terms of the implementation of

prudential standards, the performance of flights over critical infrastructure facilities has been insufficiently regulated. Of course, the introduction of geographical zones can be seen as a positive development, but in terms of flying over critical infrastructures, firstly, a limited catalogue of them is listed and only the principle of special precaution is introduced without specifying in detail how it is to be defined. The regulator could be encouraged to impose special rules for flights over all critical infrastructure and to introduce precise precautionary standards aimed at completely disqualification of threats.

With regard to intentional acts carried out for the purpose of benefiting or damaging critical infrastructure by the initiator of an attack, protective standards and solutions in this area should be considered insufficient. While the level of technology development has directly and proportionally kept pace with the increasing level of risks and the evolution of threats, the legal solutions do not sufficiently address the basic objective of critical infrastructure protection, which is to ensure continuity and thus enhance State security. The proliferation of CIP regulations may cause us to overlook the lack of consistency and dilution of regulation in the area we are discussing. Even if the general regulations on the protection of critical infrastructure are deemed to meet their objectives, standards targeted at issues related to unmanned aerial vehicles and the threats they generate are insufficient. The article points out the existence of an excellent tool for combating drones, such as interference systems, while pointing out the inadequacy of the regulations regarding its use. The very existence of the technology, as well as its effectiveness, becomes purely illusory due to the lack of legislation providing opportunities to use it. In the legislation, despite the possibility of eliminating an unmanned aerial vehicle, the responsibility for such neutralisation is not fully regulated. Furthermore, the introduced right to eliminate unmanned platforms applies to a narrow number of entities and one could reasonably postulate the introduction of this possibility for all critical infrastructure operators.

Bibliography

Adamczuk M., Cymerski J., Izak K., Kluczyński M., Krawczyk A., Maniszewska K., Olender D., Piekarski M., Rożej-Adamowicz A., Szlachter D., Tomasiewicz J., Wojtasik K., *Security of critical infrastructure in the face of threats from unmanned platforms*, Polish Society for National Security, "PTBN Report" 2021, Volume II.

Bednarczyk W., Kopczewski M., *Tasks of Public Administration in the System of Critical Infrastructure Protection*, "Scientific and Methodical Review, Education for Security" 2017, Year X, Nymer 3/2017.

Bielawski R., *Safety of Unmanned Aerial Systems in a Disturbance Environment*, "De Securitate et Defensione, On Security and Defence" 2019, no. 2 (5).

Bunsh I., Świątkowska J., *New trends in the area of critical infrastructure protection – a European perspective*, „Scientific Work of Wałbrzyska Wyższa Szkoła Zarządzania i Przedsiębiorczości" 2013, T. 25 (5).

Cheba S., Kutyła P., Mroczkowska A., Olszewska M., Szczukocki A., Szkudlarek P., Wierzbicka J., *Delivering U-Space in order to boost Poland's competitivness*, [in:], S.A. Jarecki, *Modern infrastructure as a tool to build the strength and competitiveness of the Republic, collective work*, Report of the Students of the National School of Public Administration, 2020.

Chojnacki J., Pasek D., *History of the use of unmanned aerial vehicles*, "International Security Yearbook" 2017, vol.11, no.1.

Druszcz M., *Use of unmanned aerial vehicles for the protection of critical infrastructure line installations*, "Police Review" 2018, No. 4 (132).

Górski K., Szymański S., Mielczarek I., Grzesiak J., *Electronic systems for protection against BSP*, "Electrotechnical Review" 2022, R. 98, No. 9/2022.

Karolewski A., Rejman-Karolewska M., *Protection of critical infrastructure*, "Scientific and Methodical Review, Education for Security" 2015, Year VII, Number 2/2015 (27).

Kasperkiewicz J., *Unmanned aerial vehicles (drones) and the latest draft legal regulations on their use*, "University of Warsaw Law Review" 2015, Year XIV, No. 1/2015.

Kawka W., *Conditions for using non-lethal weapons of new generation as components of critical infrastructure system in the environment of hybrid threats, Problems of Technology and Armaments*, Wojskowy Instytut Techniczny Uzbrojenia, "Journal" 2022, no. 1/2022.

Kochańczyk R., Stechnij T., Wilisowski A., Sitko P., Fellner R., *Legal and certification aspects of unmanned aerial vehicles in light of selected international rules*, Katowice 2019.

Kolano S., *Identifying threats to the state's critical infrastructure*, "Public Security" 2018, no 12/2018.

Lasota-Jędrzejak A., *Security of the State's Critical Infrastructure*, "Yearbook of Maritime Security" 2013, Year VII.

Leśniak G., Płatek P., Szmit Ł., Czyżewska M., Grązka M., Michałowski J., *Analysis of man-portable systems intercepting miniature unmanned aerial vehicles, Problems of Armament Technology*, Military Institute of Armament Technology, "Journal" 2017, no. 2/2017.

Łukasiewicz J., *Offshore wind farms as potential targets for attack using unmanned aerial vehicles*, "Government Security Centre Quarterly Bulletin" 2021, Number 32.

Łukasiewicz J., *Unmanned aerial vehicles as a source of threats to the infrastructure of the supply of electricity to countries and proposed methods of protecting this infrastructure, Terrorism – studies, analyses, prevention*, "Terroryzm – studia, analizy, prewencja" 2022, No. 1 (1), 2022.

Łukasiewicz J., Piekarski M., Kluczyński M., *Security of critical infrastructure in the face of threats from unmanned platforms*, Polish National Security Association, "PTBN Report" 2021, volume II.

Milewski J., *Identification of Critical Infrastructure and its Threats*, "Scientific Journals of Akademia Obrony Narodowej" 2016, No. 4 (105).

Modelski M., *Identification and protection of critical infrastructure in Poland*, "Scientific Journals, Lotnicza Akademia Wojskowa" 2018, No. 1-2.

Panasiuk A., Sierański S., *Protection of critical infrastructure facilities*, "State Control" 2017, No. 1.

Pietrek G., *Threats to critical infrastructure. The case of unmanned aerial vehicles*, "Journal of Modern Science" 2022, Volume 2/49/2022.

Pietrek G., *Critical infrastructure security management, Anti-drone systems,* "Defence Knowledge" 2022, Vol. 280 No.

Pietrek G., Pietrek M., *Unmanned aerial vehicles as a threat to critical infrastructure*, "Scientific Journals of Fire Service School" 2022, no. 83.

Stec K., *Selected Legal Tools for Critical Infrastructure Protection in Poland, National Security*, "Bezpieczestwo Narodowe" 2011, no. 19.

Szubrycht T., Szyma T., *Electromagnetic weapons as a new means of warfare in the information age*, "Scientific Journals of Akademia Marynarki Wojennej" 2005, Year XLVI no. 3 (162).

Wasilewski K., the Liability of the UAV Operator for the Preformed Flight, in Feltynowski M., *Use of unmanned aerial platforms in public safety operations*, Warszawa 2019.

Wyszywacz W., Safety of Air Operations in the Aspeck of Training and Work, [in:] *Use of Unmanned Aerial Platforms in Public Safety Operations*, Feltynowski M. (Ed.), Warszawa, 2019.

Act of 26 April 2007 on crisis management, consolidated text according to the Announcement of the Speaker of the Sejm (one of the chambers of the Parliament) of the Republic of Poland of 1 December 2022 on the announcement of the consolidated text of the Act on crisis management, Journal of Laws of 2023, item 122.

Act of 3 July 2002, Aviation Law, consolidated text introduced by the Announcement of the Speaker of the Sejm of the Republic of Poland of 28 April 2022, Journal of Laws of the Republic of Poland, Item 1235, 10.06.2022.

Act of 13 April 2007 on electromagnetic compatibility, Journal of Laws of 2019, item 2388, as amended.

Act of 16 July 2004. Telecommunications Law, Journal of Laws 2019, item 2460, as amended.

Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aerial systems and operators of unmanned aerial systems from third countries, Journal of Law L152 of 11.06.2019.

Commission Implementing Regulation (EU) No. 2019/947 of 24 May 2019 on rules and procedures for the operation of unmanned aerial vehicles, Journal of Laws L152 of 11.06.2019.

Guideline No. 7, President of the Civil Aviation Authority, on ways to perform operations with using systems unmanned aircraft in connection with entry into force provisions of Commission Regulation (EU) No. 2019/947 of on 24 May 2019 on regulations and procedures for operation of unmanned aircrafts, 9 June 2021, Item 35.

Guideline No. 24, President of the Civil Aviation Authority, Official Journal of the Civil Aviation Authority, on designation of geographic zones for unmanned aerial vehicle systems, 30 December 2020, pos. 78.

National Standard Scenario NSTS-01 – Guidance Note No. 15 on National Standard Scenario NSTS-01 for visual line of sight (VLOS) or first-person view (VPV) operations using an unmanned aerial vehicle with a take-off mass of less than 4kg, Official Journal of the Civil Aviation Office, 30 December 2020, item 69.

National Standard Scenario NSTS-02 – Guidance Note No. 16, on National Standard Scenario NSTS-02 for visual line of sight (VLOS) operations using unmanned aerial vehicles in the multi-rotor (MR) category with a take-off mass of less than 25kg, Official Journal of the Civil Aviation Office, 30 December 2020, item 70.

National Standard Scenario NSTS-03 – Guidance Note No. 17, on National Standard Scenario NSTS-03 for visual line of sight (VLOS) operations using unmanned aerial vehicle in fixed-wing category (A) with a take-off mass of less than 25kg, Official Journal of the Civil Aviation Office, 30 December 2020, item 71.

National Standard Scenario NSTS-04 – Guidance Note No. 18, on National Standard Scenario NSTS-04 for visual line of sight (VLOS) operations using unmanned aerial vehicle in the helicopter (H) category with a take-off mass of less than 25kg, Official Journal of the Civil Aviation Authority, 30 December 2020, item 72.

National Standard Scenario NSTS-05 – Guidance Note No. 19, on National Standard Scenario NSTS-05 for Beyond Visual Line of Sight (BVLOS) operations using unmanned aerial vehicle with a take-off mass of less than 4kg, within 2km of the pilot of the unmanned aircraft, Official Journal of the Civil Aviation Office, 30 December 2020, item 73.

National Standard Scenario NSTS-06 – Guidance Note No. 20, on National Standard Scenario NSTS-06 for beyond visual line of sight (BVLOS) operations using unmanned aircraft in the multi-rotor (MR) category with a take-off mass of less than 25kg, within 2km of the pilot of the unmanned aerial vehicle, Official Journal of the Civil Aviation Office, 30 December 2020, item 74.

National Standard Scenario NSTS-07 – Guidance Note No. 21, on National Standard Scenario NSTS-07 for Beyond Visual Line of Sight (BVLOS) operations using unmanned aircraft in fixed-wing category (A) with a take-off mass of less than 25kg, within 2km of the pilot of the unmanned aerial vehicle, Official Journal of the Civil Aviation Office, 30 December 2020, item 75.

National Standard Scenario NSTS-08 – Guidance Note No. 22, on National Standard Scenario NSTS-08 for Beyond Visual Line of Sight (BVLOS) operations using unmanned aerial vehicle in the helicopter category (H) with a take-off mass of less than 25kg, within 2km of the pilot of the unmanned aerial vehicle, Official Journal of the Civil Aviation Office, 30 December 2020, item 76.

National Standard Scenario NSTS-09 – Guidance Note No. 21, on National Standard Scenario NSTS-07 for Beyond Visual Line of Sight (BVLOS) operations using unmanned aerial vehicles with a take-off mass of less than 25kg, performed by operators of unmanned aerial vehicle systems holding a national permit to fly (BVOLS), Official Journal of the Civil Aviation Office, 30 December 2020, item 77.

Regulation (EU) of the European Parliament and of the Council of 4 July 2018, 2018/1139 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency. Aviation Safety and amending Regulations of the European Parliament and of the Council (EC) No. 2111/2005, (EC) No. 1008/2008, (EU) No. 996/2010, (EU) No. 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council and repealing Regulations (EC) No. 552/2004 and (EC) No. 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No. 3922/91, Official Journal of the European Union L212/1 of 22.08.2018.

Regulation of the Council of Ministers of 30 April 2010 on plans for the protection of critical infrastructure, Journal of Laws of 2010, No. 83, item 542.

Resolution no. 210/2015 of the Council of Ministers of 2 November 2015 on the adoption of the National Programme for the Protection of Critical Infrastructure, with consideration of Resolution No. 116/2020 of the Council of Ministers of 13 August 2020 amending the resolution on the adoption of the National Programme for the Protection of Critical Infrastructure and Resolution No. 38/2023 of 21 March 2023 amending the resolution on the adoption of the National Programme for the Protection of Critical Infrastructure.

SORA – Specific Operation Risk Assessment, is a methodology for creating a risk analysis by which an operator flying an unmanned aerial vehicle verifies the aerial operation for safe performance. Published in AMC1 to Commission Implementing Regulation (EU) No 2019/947 of 24 May 2019 on rules and procedures for the operation of unmanned aerial vehicles. Journal of Laws L152 of 11.06.2019.

The PDRA is a simplified form of operator risk analysis proposed by the European Union Aviation Safety Agency (EASA). Where the planned operation falls within the published PDRA, the instructions contained therein can be followed while waiving the preparation of a full risk analysis. https://www.easa.europa.eu/en/document-library/easy-access-rules/easy-access-rules--unmanned-aircraft-systems-regulations--eu (accessed 17.05.2023).

The LUC Certificate is issued upon fulfilment of the conditions set out in paragraph 1, Part C, UAS.LUC.050, to Commission Implementing Regulation (EU) No 2019/947 of 24 May 2019 on rules and procedures for the operation of unmanned aerial vehicles. Journal of Laws L152 of 11.06.2019.

https://airspace.pansa.pl/map Map of geographical zones Polish Air Navigation Services Agency.

https://droneradar.eu/ Map of geographical zones of the DroneRadar.

https://drony.ulc.gov.pl/.

https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej National Programme for the Protection of Critical Infrastructure for 2023.

About the Authors

Radosław Gross, PhD student, Member of the Management Board of the company Aviacom Project sp. z o.o., Pilot UAP, Pilot UAVO.

Rui Albuquerque, PhD, Professor at the Lusófona University. Deputy Director of First-cycle political science and electoral studies.