

GRZEGORZ PIETREK *

Uniwersytet Przyrodniczo - Humanistyczny w Siedlcach, Polska

CRITICAL INFRASTRUCTURE SECURITY MANAGEMENT ANTI-DRONE SYSTEMS



ABSTRACT: The problem area outlined in the article is the existence and effectiveness of anti-drone systems used to protect the state's critical infrastructure (CI). For the purposes of the study, the following research objective was defined: assessment of the possibility of introducing anti-drone systems in critical infrastructure entities. In the next stage, the following research problem was defined: What are the needs and possibilities of developing and applying anti-drone systems to protect the state's critical infrastructure? The following sentence was adopted as the research hypothesis: Due to the growing threats generated by drones, CI protection systems are needed against them, it is necessary to develop and put into use effective anti-drone systems. In order to achieve the outlined goals, solve problems and verify research hypotheses, the author mainly used the following theoretical methods: literature analysis, legal acts analysis, synthesis, analysis (inductive and deductive), abstraction, comparison and inference. The inference was based on the SWOT analysis, a method from the group of strategic management.

KEYWORDS: critical infrastructure, security management, drones.

INTRODUCTION

The development of various types of hazards is an obvious consequence of the increase in technological advancement. Threats to people, property and the environment are divided into various categories. In this maze of different definitions, criteria and concepts we can also find some, which refer to the security of critical infrastructure. After analysing the available

* dr hab. Grzegorz Pietrek, Siedlce University of Natural Sciences and Humanities, Siedlce, Poland

 <https://orcid.org/0000-0003-2660-8025>  grzegorz.pietrek@uph.edu.pl

literature and familiarising oneself with the current legal acts, one may come to the conclusion that one of the threats which has appeared relatively recently but seems to be significant and "developing" is the threat from "Unmanned Aerial Vehicles", commonly known as drones.

An Unmanned Aerial Vehicle, in its simplest definition, is a machine that does not require a crew present on board in order to fly, does not have the ability to carry passengers and is piloted remotely or flies autonomously. In fact, the aircraft itself needs additional resources and equipment to operate. These devices communicate with each other and enable the aircraft to perform its task.

This article is intended to indicate and highlight the need for the introduction into common use of anti-drone systems to protect the critical infrastructure of the state. The Act on crisis management permanently and invariably includes among the elements constituting critical infrastructure the following systems: (1) supply of energy, energy resources and fuels; (2) communication; (3) information and communication networks; (4) financial; (5) food supply; (6) water supply; (7) health protection; (8) transport; (9) rescue; (10) ensuring continuity of public administration; (11) production, storage, storage and use of chemical and radioactive substances, including pipelines of hazardous substances².

The available literature indicates that anti-drone systems are being developed, there are various configurations and application possibilities. It can also be noted that there is a multiplicity of solutions and the possibility of "selecting" an "anti-drone" solution appropriate to the specifics of a particular critical infrastructure system.

ORGANIZATIONAL CONDITIONS OF CRITICAL INFRASTRUCTURE IN POLAND

The National Programme for Critical Infrastructure Protection (NPOIK) - in accordance with Art. 5b (1) of the Act on Crisis Management - is a document which aims to create conditions for the improvement of critical infrastructure security. NPOIK defines the principles of critical infrastructure (CI) protection and the cooperation of CI owners with public administration. It is an innovative and unique document. Its uniqueness lies, inter alia, in its unsanctioned approach to critical infrastructure protection based on trust and cooperation between public administration and the owners and holders of CI facilities. The content of the programme derives directly from the provisions of the Act on crisis management and the definition of

² Legal Act - Ustawa z dn. 27 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. 2007 nr 89 poz. 590., Art. 3, ust. 2.

critical infrastructure contained therein, which makes it possible to assess which facilities, devices, installations and services are crucial for the security of the state and its citizens, and also serve to ensure the efficient functioning of public administration bodies, institutions and entrepreneurs.

The Act defines national priorities and standards in the scope of their protection, in terms of responsibility of the government administration, self-government administration and services established to ensure national security, and while establishing them the key criterion is their importance for undisturbed functioning of the state and security of citizens.

The aim of the National Programme for Critical Infrastructure Protection is to create conditions for improving the security of CI, in particular with regard to: (1) preventing disruptions to the functioning of critical infrastructure; (2) preparing for crisis situations that may adversely affect critical infrastructure; (3) responding destruction or disruption of critical infrastructure; (4) Restoring critical infrastructures³.

The programme distinguishes five basic approaches to critical infrastructure protection⁴:

a) Physical protection - a set of measures which minimize the risk of disruption by persons found in critical infrastructure without authorization. This includes protection of persons and protection of property, as well as prevention of damage and prevention of unauthorised access to protected areas.

(b) Personnel protection - a set of undertakings and procedures aimed at reducing the risk associated with persons who, through authorised access to CI facilities, equipment, installations and services, may cause disruption to its functioning. This protection should therefore be related to employees and other persons temporarily present within the critical infrastructure.

(c) Technical protection, which includes matters relating to the compliance of buildings, facilities, installations and services with applicable standards (e. g. construction) as well as other legislation (e. g. fire) to ensure the safe use of critical infrastructure and the technical protection of the site, i. e. the use of fences, barriers, CCTV systems, access systems, and similar measures.

³<https://rcb.gov.pl/narodowy-program-ochrony-infrastruktury-krytycznej-przyjety-przez-rade-ministrow-2> (accessed: 29. 07. 2021).

⁴ Ibidem.

d) Information and Communication Technology Protection for critical infrastructure systems and networks - this also means protection against cybercrime and cyber-terrorism, and the prevention of such incidents.

e) Legal Protection - a set of measures aimed at minimising the risk of other business, public or private entities, whose activities may lead to a disruption of critical infrastructure facilities, equipment, installations and services.

The Annex to the Programme also defines criteria to identify facilities, installations, equipment and services forming part of critical infrastructure systems. Together with a uniform list of critical infrastructure, these criteria were developed and updated by the Government Centre for Security in cooperation with ministers and heads of central offices responsible for individual systems.

It is worth noting that the authors of the document have also identified weaknesses in the procedure of imposing obligations on operators of critical infrastructure by way of laws or regulations, due to the real lack of possibility to audit and control their implementation. With this in mind, the entities that manage CI should be more involved in activities in the field of CI protection - not only through orders, but also through conscious participation in undertakings aimed at improving the security of systems important for the functioning of society by intensifying cooperation between the private and public sectors in this field⁵.

The main objective of the Program is to create conditions for improving the safety of CI. Together with other program documents it constitutes the primary objective - improvement of the security of the Republic of Poland - in this respect the document does not differ from the previous edition. However, significant quantitative differences occur at the stage of formulating intermediate (detailed) objectives. These objectives provide for: the acquisition of a specific level of awareness, knowledge and competence of all participants in the Program regarding the importance of CI for the efficient functioning of the state and the ways and methods of its protection; the introduction of risk assessment methodology taking into account the full range of threats, including the methodology of dealing with threats of very low probability and catastrophic effects; the introduction of a coordinated and risk-based approach to the implementation of tasks in the area of CI protection; building partnerships between the participants of the CI protection process; the introduction of mechanisms for the

⁵ Legal Act: Uchwała nr r 67 Rady Ministrów z 9 kwietnia 2013 r. w sprawie przyjęcia „Strategii rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022”, Monitor Polski z 16 maja 2013 r., poz. 377.

exchange and protection of information provided between the participants of the CI protection process⁶.

The basis of this understanding of the protection system is the authors' assumption that increasing the effectiveness of CI protection can only occur through the actions of its operators supported by the capabilities and capacities of the public administration⁷.

Unfortunately, sanctionlessness is also associated with the lack of financial support for critical infrastructure operators, which is presented as a balancing factor between the sovereign influence of the state and the expenditures necessary to improve the security of CI. It was thus reminded that the Crisis Management Act does not provide for sanctions for failure to comply with the obligations set out therein, nor does it provide for budgetary support for CI operators⁸ and a catalogue of principles was presented as guidelines for implementing the Program objectives by its recipients. Among them the following were identified as the most important pillars: joint responsibility understood [...] as a common (collective) effort to improve CI safety resulting from the awareness of its importance for the functioning of public administration bodies and CI operators, society, the economy and the state. Protecting critical infrastructure is in the interest of both its operators and the administration responsible for the functioning of the state⁹; cooperation means the performance of specific, converging and complementary tasks together by the participants in CI protection in order to achieve a common goal that stems from the principle of shared responsibility. Cooperation is necessary in order to avoid duplication of actions and costs and to use available forces and resources more efficiently.¹⁰; trust - the third pillar of the CIP regime - understood as the belief that the motivation of CI protection participants (in administration and CI operators in particular) is to strive for a common goal - improving the security of CI and the Republic of Poland. Achieving this goal will therefore benefit all stakeholders, including society in particular¹¹.

A synthetic summary of the opportunities and threats to critical infrastructure security management that arise from the National Program for Critical Infrastructure Protection is shown in Table 1.

⁶ Ibidem.

⁷ Ibidem.

⁸ Ibidem.

⁹ Ibidem.

¹⁰ Ibidem.

¹¹ Ibidem, p. 10.

Table 1

Opportunities and threats for critical infrastructure security management resulting from the National Program for Critical Infrastructure Protection

Opportunities	Threats
<p>-Developing clear rules and procedures between state authorities and services and owners and possessors of intrinsic and tangible property, installations or equipment of critical infrastructure;</p> <p>-Recognizing CI protection as a process geared towards safeguarding the continuity of a particular service and its restoration in case of need;</p>	<p>- cross-sectoral partnership means only a limited form of cooperation between public administration units and private entities, though, for example, exchanging any information which may affect the attainment of the NPOIK objectives; such partnership does not, however, provide for the conclusion of any agreement pursuant to which a private partner would carry out, for remuneration, a project for the benefit of the public entity</p> <p>- identifying weaknesses in the procedure for imposing obligations on critical infrastructure operators through laws or regulations due to the real lack of possibility to audit and control their implementation.</p>

Source: Authors' own study

The National Program for Critical Infrastructure Protection, together with its annexes, is a document which provides basic information on the technical and organizational aspects of critical infrastructure protection and serves as a set of specific guidelines for the construction and functioning of a critical infrastructure protection system to prevent selected threats. Due to the miniaturization of electronic drones, which are used for reconnaissance and information acquisition, but also as effectors used for example in the Ukrainian conflict, threats are increasing.

Table 2 provides a kind of extract from the available reports (The Global Risk Report) for the years 2021 and 2022, which refer to possible threats to the security of critical infrastructures and determine their level of impact on the security management of these systems.

Table 2.

Estimated level of impact on critical infrastructure security management from threats

Threats	Low	Medium	High
Extreme weather phenomena		X	
Failure of a cyber-security system			X
Terrorist attacks			X
Breakdown of IT infrastructure			X
Weapons of mass destruction		X	
Collapse of the state	X		
Unfavourable technological development		X	
Forced migration	X		
A breakdown in inter-state relations	X		
Geophysical disasters			X

Source: Own elaboration based on the following reports: WEF_The_Global_Risks_Report_2021.pdf, WEF_The_Global_Risks_Report_2022.pdf.

SAFETY RISKS RELATED TO THE USE OF DRONES

Unmanned aerial vehicles (UAVs), commonly known as drones, are a natural consequence of technological development. UAVs can be used for research, rescue, measurement and diagnostic purposes, supporting humans in their efforts to improve safety and quality of life. However, like all technological advances, UAVs can also be used in a way that will threaten human health and life, property or the environment.

Drones are becoming available to everyone, and their price in terms of flight performance and weight is getting lower and lower. This results in the widespread use of drones and, at the same time, the generation of an increasing number of risks, which can be broadly categorized as follows¹²:

- Transport including air traffic (collision between UAV and vehicle, aircraft or diversion of driver's attention);
- Terrorism (security of transport and critical infrastructure, densely populated areas, mass events);
- Smuggling (borders - bypassing checks, special protection facilities);
- Threats to property;
- espionage (invasion of privacy, industrial espionage, wiretapping, spying on institutions and public figures, government agencies, military installations);

¹² R. Fellner, A. Mańka, *Kursy operatorów bezzałogowych statków powietrznych - "Prawo jazdy na drony (UAV)"*, www.bsp.2ap.pl, www.ktl.polsl.pl, (accessed: 2. 08. 2021).

- Invasion of privacy (noise, discomfort, sense of danger);
- Environmental hazards (noise, fire, disturbance of wildlife)¹³.

The official breakdown of UAVs is relevant in terms of the need for a license. UAVs for conventional purposes have a maximum take-off mass (MTOM) of up to 25 kg. However, this range is subdivided by regulation into¹⁴: UAV up to 2 kg; UAVs from 2 to 7 kg; UAVs from 7 to 25 kg¹⁵.

The threats from a UAV operating autonomously and programmed to fly around designated GPS points are much greater due to its ability to operate without RC equipment and the lack of detection of this type of communication. Extremely high risk in moving unmanned vehicles also involves sharing the flight space with other objects. The greatest danger to humans here is with land and air vehicles. Knowledge of road traffic law is much more common than knowledge of the rules on the use of shared airspace under aviation law. A collision between an unmanned vehicle and a vehicle carrying people can result in damage and an emergency landing. For example, UAVs used amateurishly to observe a fire have forced firefighting helicopters to a higher flight ceiling, making it impossible to accurately drop water¹⁶.

Unmanned vehicles pose a serious threat especially to aircraft engines and - indirectly - to their operators. Just sharing airspace while maintaining height separation is a challenge. A very high hazard, both for operators of multi-rotor UAVs and for bystanders, is posed by rotating components. This danger is mainly present in the heavier flying vehicles and in some waterborne vehicles. They are posed by rapidly rotating propellers that can cut the skin and can damage important arteries in the human body. UAVs are also often used commercially to monitor mass events such as gatherings or concerts. As technical devices, they can fail, resulting in very serious consequences. A vehicle weighing about 5 kg and hovering at a height of 30 m has a potential energy of about 1.5 kJ. This energy is enough to break the thickest of human bones and poses a lethal threat to those on the ground directly below the vehicle¹⁷.

¹³ Ibidem.

¹⁴ Legal act: Rozporządzenie (UE) 2018/1139 w sprawie wspólnych zasad w dziedzinie lotnictwa cywilnego i utworzenia Agencji Unii Europejskiej ds. Bezpieczeństwa Lotniczego.

¹⁵ *Drony w służbie społeczeństwa*, „Innowacje techniczne”, 2016 <https://iq.intel.pl/drony-w-sluzbie-spolnoczenstwa/> (accessed: 20. 07. 2021).

¹⁶ N. Tuśnio, A. Nowak, J. Tuśnio, P. Wolny, *Bezzałogowe statki powietrzne w działaniach Państwowej Straży Pożarnej – propozycja dedykowana Państwowej Straży Pożarnej*, Zeszyty Naukowe SGSP 2016, 58, tom 1/2.

¹⁷ P. Polkowski, *Bezzałogowe statki powietrzne unmanned aerial vehicles*, „Rocznik Bezpieczeństwa Międzynarodowego” 2016, 10(1).

An unmanned aircraft, in its simplest definition, is a machine that does not require a crew on board to fly, does not have the capacity to carry passengers and is piloted remotely or flies autonomously. In fact, the aircraft itself needs additional resources and equipment to operate. These devices communicate with each other and enable the aircraft to perform its task¹⁸.

A UAS (Unmanned Aerial System) consists of the following components ¹⁹: UAV - an unmanned aircraft; a ground control station (GCS), operated by the operator; a communication system between the control station and the aircraft in the air; an interchangeable payload, used depending on the nature of the mission to be performed; software to process the data collected; auxiliary equipment, for transport and operation of the entire system.

The field of drones - the multi-rotor aircraft that have gained the most popularity in recent years, when flying make a characteristic sound produced by rapidly spinning propellers, similar to flying drones. Unmanned Aerial Vehicles can be divided into several categories, depending on construction and propulsion: multi-rotors, airframes, helicopters and hybrids.

The unmanned aircraft is equipped with various types of effectors (radar sensors, optoelectronic heads, spectrum analyzers, acoustic sensors), which serve to: observation, information transfer and enemy missile strike. The device can also be used as a simple aircraft transporter to carry explosives, weapons, poisonous agents or to smuggle drugs across national borders. The device itself, in contact with another traffic participant, aircraft or car poses a serious threat to airports, highways or other critical infrastructure etc. Despite the flight ban, there are cases of notorious violations. Drones are flying devices that move at low speeds and low altitudes, making them difficult to detect. In addition, they have a very small effective reflective surface, as a result of which they are very difficult to recognise by radar. It also becomes a problem to determine the owner or pilot of the vessel. This is because it can be controlled from a distance using, for example, the LTE internet network. This can be done from a laptop from anywhere in the world. With the development of technology, regulations regarding aviation law are being changed, which today forbids steering without a license, unless its weight does not exceed 0.6 kg. An unmanned aircraft can be used in a positive sense as surveying or taking aerial photographs. However, there is a danger that the control signal may be intercepted and the UAV changes ownership.

¹⁸ Holliday B., *Drones: The Complete Collection*, CreateSpace Independent Publishing Platform, 2017, s. 123.

¹⁹ <https://bzbuas.com/blog/aktualnosci/co-to-jest-uav-uas-bezalogowe-statki-powietrzne/> (accessed: 7. 08. 2021).

Today's drone used against critical infrastructure poses a challenge to it. Drones are very quiet, cannot be heard or seen, and are capable of spying on technical infrastructure. It is important to be aware that the airspace around critical infrastructure is the least secure and it is practically possible to fly with impunity through the use of UAVs.

Table 3. identifies the most real risks associated with drone use and their impact on the security management of critical infrastructure systems

Table 3.
Estimated level of impact of drone use on critical infrastructure security management resulting from the classification

Threats	Low	Medium	high
Terrorist attack (incl. weapons of mass destruction)			X
Surveillance			X
Smuggling	X		
Accidents (collisions with another object, falls)			X
Events involving VIPs (assassination)	X		

Source: own study.

This part of the study focuses primarily on performing a risk analysis according to three variables: probability of occurrence, vulnerability and strength of impact (effect). This analysis aims to assess the risk of the impact of Unmanned Aerial Vehicles on the preservation of the continuity of the State's critical infrastructure through the prism of the realization of the national interest. This assessment is quantitative in nature.

Table 8:

Risk analysis of the impact of BSL on CI business continuity

Elements of the analysis	Hazard/disruptive symbol	Likelihood of occurrence (from 1 to 5)	Vulnerability (from 1 to 3)	Strength of influence/impact (from 1 to 5)	Risk Assessment	Risk acceptance level
1	2	3	4	5	6 (3x4x6)	7
Energy, raw materials and fuels supply systems	1	5	3	5	75	75
Communication systems	2	5	3	5	75	75
ICT network systems	3	5	3	5	75	75
Financial systems	4	3	2	2	18	18
Food supply systems	5	2	1	2	4	4
Water supply systems	6	4	2	4	32	32
Health care systems	7	1	1	2	2	
Transport systems	8	4	3	4	48	48
Rescue systems	9	2	1	2	4	4
Business continuity systems for public administrations	10	2	2	3	12	12
Systems for production, storage, containment and use of chemical substances and radioactive substances, including pipelines for dangerous substances	11	5	3	5	75	75

Source: own study.

Description:

Probability

- 1 - very low (unlikely);
- 2 - low (rare);
- 3 - medium (possible);
- 4 - high (probable);
- 5 - very high (very likely);

Vulnerability to hazards, events

- 1 - low;
- 2 - medium
- 3 - high;

CI's vulnerability to threats/events depends on the level of acquisition of resources, processes: e.g. recruitment system, level of dependence on stakeholders.

Impact/impact is determined by the magnitude of possible financial and non-financial (e.g. image) losses

- 1 - negligible
- 2 - small
- 3 - medium
- 4 - large;

5 - catastrophic.

Risk assessment:

Extreme: above 60 - 75 points.

Great: 45 - 60 points.

Medium: 30 - 45 points.

Low: 15 - 30 points.

Minimal: below 15 points.

Risk acceptance level:

unacceptable risk: over 70 points.

tolerable risk: 46 to 59 points.

permissible risk: between 15 and 45 points.

acceptable risk: below 15 points.

The analysis presented above shows that vulnerable and high potential for drone threats are critical infrastructure such as: energy, energy commodity and fuel supply systems; communication systems; ICT network systems, systems for production, storage, storage and use of chemical and radioactive substances, including pipelines for hazardous substances. In these cases the risks are unacceptable. Rescue systems are also high risk, but to a lesser extent than those indicated above. The remaining systems are in the the "acceptable" risk group.

Nowadays, the security of critical infrastructure not only constitutes the basis of state operation, but is actually a sine qua non for its functional existence. Therefore, the public administration undertakes actions aimed at the most effective protection of services, without which it is difficult to imagine a modern state. One of the key elements of these activities is undoubtedly the creation of an appropriate regulatory environment. Critical infrastructure legislation must address three main challenges²⁰: Predicting the type and severity of a potential crisis that might adversely affect critical infrastructure; ensuring that appropriate crisis response tools are in place; and maintaining the proportionality of the tools created, by maximising the protection of public safety and minimising the negative impact on individual liberties.

²⁰ J. Zawila - Niedźwiecki, *Ciągłość działania organizacji*, „Prace Naukowe Politechniki Warszawskiej. Organizacja i Zarządzanie Przemysłem”, 2008/z. 20 / 3 – 107, s. 32.

Organisations operate in a rapidly changing environment, under constant pressure from the need to constantly reduce operating costs and protect themselves from potential disruptions. The fulfilment of these tasks through the possession of modern technical infrastructure, improvement of the qualifications of the employed staff, compliance with norms and legal acts and similar continuous competition has become a reason for the emergence of operational threats. In connection with this as a result, we hear more and more about business continuity management, which is aimed at determining the potential impact of disruptions on the organisation and creating conditions for building resilience to them, as well as creating the conditions for the development of business continuity management. That helps to act effectively in terms of protecting the key interests of the organisation's owners, reputation and brand, as well as the values achieved in its previous activities, i. e.²¹:

- guarantee the liquidity of business processes;
- minimize the threat of loss of critical assets;
- minimize time and energy wasted on restoring proper business processes or recovering lost resources;
- manage the company's quality and image;
- avoid legal consequences resulting from non-compliance with applicable regulations.

Obtaining full knowledge of all threats is practically impossible. Mainly because the variety of phenomena posing a threat to the achievement of the intended objectives by the company is enormous. These threats arise in various organisational - legal, economic - financial, technical and technological and other conditions. This means the emergence of new types of risk and metamorphosis of the existing ones.

The logical response of the organisation to disturbances is to build a homeostasis mechanism based on monitoring threats, neutralising them, and when this fails, restoring the state before the disturbance, and until then providing forms of substitute action. Such behaviour is an expression of a rational response to an unavoidable risk. Detailed analysis of the mechanism of such behaviour leads to the identification of criteria for rational risk assessment and model response attitudes, appropriate to the magnitude of the potential impact of the risk. In particular, the rationality of the response is based on an assessment of

²¹ Ibidem, s. 33.

risk intensity factors, i.e. the strength of the impact of the risk (especially potential damage) and the frequency of impact²².

Business continuity, firstly, is a postulate of excellence of the system of operation, which is every organisation, and therefore every economic or administrative entity. In this sense, ensuring business continuity is the subject of strategic management, expressing the primary objective of organisational efficiency and taking primacy in the area of operational risk management.

Secondly, business continuity is understood as an organisational behaviour that creates the capacity of an organisation to respond effectively in a situation of disruption resulting from the peculiar interaction of manifestations of threat with the vulnerability of the internal organisation, infrastructure or resources. In this sense, ensuring business continuity is the subject of operational management and is the last link of operational risk management.

Generally speaking, business continuity is the ability of an organisation to respond to disruptions to the conditions for normal operations in such a way that, where possible, these normal conditions are quickly restored, and where this is not possible, to move on to a planned method of substituting tasks. Business continuity is thus viewed, both in the context of the organisation's tasks and the processes for achieving those tasks, and in the context of the factors that can disrupt those processes and the forms of vulnerability of the organisation that make it susceptible to disruption.

Ensuring business continuity includes²³:

- organisation's mechanism of reacting to disturbances;
- the process of developing the aforementioned mechanism of capability to respond to disruptions (as a process - in the sense of process analysis - the core activity of the organization);
- the process of managing the current business continuity capability and its continuous improvement.

The interference response mechanism consists of²⁴: an organisational structure dedicated to the task of ensuring continuity, forming a coherent whole with the overall organisational structure; formal organisational arrangements defining the relationships in the organisational

²² Ibidem, s. 34.

²³ Ibidem, s. 39.

²⁴ Ibidem .

structure related to the task of ensuring continuity; established practice (possibly written down) of acting in situations when a response to a disturbance is required.

First of all, it should be emphasised that responding to disruptions by ensuring business continuity should be understood not only as a direct action against disruptions, but also as an activity of preventive character, connected with the analysis of threats and vulnerability analysis and the search for methods and solutions to prevent the occurrence of disruptions.

In this sense, business continuity and security efforts are intertwined. From a business continuity point of view, security solutions ensure the prevention of threats, while from a security point of view, business continuity solutions provide additional security. This justifies the concept of joint management of both issues, and likewise quality management²⁵.

The threat of unmanned aerial vehicles to critical infrastructure is real. Drones are a fresh topic, but the technology market is already advanced enough that newer and more refined designs are emerging. As a result, it could pose a problem for even the most modern anti-drone systems.

Potential terrorists who launch attacks on CI facilities are most likely to use very light or lightweight drones. These are available almost everywhere and without any major problems. They are also not troublesome to operate, and their price is low enough that even their destruction in the failure of a potential terrorist act is not felt in any way. While lightweight drones will not carry heavy payloads, it is well known that just a small amount of anthrax bacteria is capable of killing many people. A digital camera can also be attached to the drone, allowing potential terrorists to see the topography of the area of the particular CI facility they are targeting.

One of the biggest threats to CI is the chemical threat. Penetration of dangerous viruses and bacteria into groundwater or large water reservoirs exposes large numbers of people to loss of health or even life. A drone may carry a dangerous substance (e. g. viruses or bacteria) over a larger group of people (e. g. during mass events or demonstrations). Another example could be the appearance of a drone with a small explosive charge, e. g. over an airport or a large tank of petroleum substances in a fuel base. Unnoticed, a small unmanned flying object can paralyse the traffic of an airport or put people's health and lives at risk by planting a charge in an oil port, which in addition brings huge financial losses.

²⁵ Ibidem.

Unmanned aerial vehicles equipped with good optics with image recording (either on an internal disk or with the ability to transmit the image directly to the operator) could be used by potential terrorists to produce a location map of the point on which an attack would be most noticeable and cause the most damage. An attack on a facility in the oil and energy industry would have such an effect. For example, during a terrorist attack using a drone on the energy sector, a so-called blackout could occur, i. e. a lack of voltage in the power grid over a significant area²⁶.

REDUCING THE RISK OF HAZARDS

Several technical solutions already exist on the market to detect an approaching UAV. These include²⁷:

1) Audio detection - involves the detection of characteristic frequencies in the infrasound range. These are emitted, for example, by the rotation of propellers and are collected by the system in the form of a digital interpretation of the acoustic signal. These are called acoustic signatures. The more signatures in the device's software database, the more accurately the drone is identified. However, the low amplitude of the sounds emitted by the drone, as well as the frequently occurring background sound, affect the detection distance. This is usually a maximum of around 50 m with average external interference in the form of additional background noise.

2) Video detection - is based on detecting movement of an object against a static image (such as a terrain image). There are many algorithms of motion detection. The problem is primarily a small difference in contrast between the drone and the background and the sheer size of the UAV in relation to the size of the image. It should be noted that with a constant focal length of the camera lens at longer distances, the image from the UAV occupies a smaller section of the camera sensor (fewer image pixels). In extreme cases it can be one pixel. Variable focal length lenses can of course be used. However, with a large focal length the viewing angle of the camera is very narrow both vertically and horizontally, so the field of observation decreases (but the distance of this field from the sensor increases). With large lens focal lengths it is also very difficult to maintain stability of the system, which causes that the whole image is moving and does not have fixed points, and can also be blurred and out of focus. This results in

²⁶ <http://www.anti-drone.pl/informacje/zagrozenia> (accessed: 6. 08. 2021).

²⁷ <http://www.anti-drone.pl/informacje/rozwiazania> (accessed: 7. 04. 2022).

a lack of recognition or identification. When using video cameras as a detection method, its range is currently around 100m. Depending on the solution, the camera software may mistakenly identify any movement as that of a UAV. An example would be birds, which the system identifies as UAV under certain circumstances. This affects the number of false alarms that can be generated by the system.

3) Thermal imaging - this is a thermal image of the observed object. The important factor here is the amount of heat produced by the flying vehicle depending on the type of propulsion used. However, only drones of large size are perfectly visible. For available civil/recreational drones, the range of this detection method is currently only about 100 m. The undoubted advantage of this solution is the possibility to observe objects in total darkness and at low air transparency (fog, precipitation). The downside, however, is the very high probability of such a UAV being considered a bird.

4) Radar - radio waves reflect differently depending on the wavelength, shape and effective reflective area of an object. The radar search area is the space limited by the maximum and minimum detection distance and the width of the azimuth and elevation angle sector. In the case of detection of small objects, such as drones, with this method, the problem is the influence/harm of the used wavelength on living organisms, as well as the detection of a large number of objects, and thus the number of false alarms, e.g. due to birds. An advantage may be a large detection distance. Undoubtedly, the functionality of such a system is also influenced by terrain, which for the radar system to work properly must be free of any terrain obstacles.

5) Radio waves - civilian drones can fulfill their tasks using radio communication, in available bands (e.g. 5.8 GHz). This is used not only for communication and execution of operator commands, but also to perform other functions needed to ensure the operation of the device. Currently, it is the basic way to control this type of devices, in the bands allowed and accepted for all. Thanks to the detection of radio signals, apart from an alarm about the appearance of a drone, it is possible to obtain other information which is important from the point of view of protection, e. g. precise coordinates of the object as well as its operator (who can control the drone from hiding), identification of the type of device. Depending on the type of detector used, the detection distance is up to several kilometers.

Each of the above mentioned methods of detection is characterised by varying effectiveness in terms of detecting unmanned aerial vehicles. This effectiveness translates directly into the response time of the services responsible for protecting a given area, such as

an airport, a railway station or a public facility. It should be remembered that UAV are not subject to typical limitations encountered in road communication, so they can cover space directly along a straight line leading to the target. Additionally, they are distinguished by their high speed in covering a set distance. A typical UAV used only for recreational purposes can successfully reach speeds of 100 km/h and more.²⁸.

The above considerations clearly point to two separate issues related to of using a UAV to commit an act of unlawful interference, which significantly affect the security of a public facility. These are threat detection and neutralisation.

Due to the speed at which an unmanned aircraft moves, if a threat is identified there is a need for an almost immediate response to eliminate it. At present, manufacturers compete in developing so-called anti-drone systems, which are characterised by varying effectiveness of the techniques used to neutralise the UAV. The most popular proposed methods for eliminating the threat posed by an approaching UAV can be classified as follows²⁹:

a) laser warhead - currently 1-2 kW systems are being tested, typically for small drones. The principle of operation is as follows: detection of the target, then heating the drone element with a laser beam until it ignites and crashes.

Due to its military importance, this solution is not available to customers other than the armies of the countries where the devices are manufactured.

b) missiles - the detection of a BSP by radar launches a missile which is guided to the target by a tracking system. The best known solution of this type is EAPS ID. This is a military-only technology developed and used mainly for other purposes than just destroying small drones.

c) interception of a BSP in the air by another flying object - the basic principle of these systems is that the interceptor drone arrives in the vicinity of the intruder drone. The distance between them determines the type of solution (netting, throwing ribbons in the propellers, firing plastic balls).

d) gunshot - effectiveness is influenced by the type of weapon used, the conditions under which the shot was fired and the behaviour of the drone before impact (e. g. size and speed). In most incidents drones shot down by firearms were hovering or moving relatively slowly.

²⁸ <https://www.cnbop.pl/wydawnictwa/ksiazki/978-83-948534-6-4/wykorzystanie-bpp-w-operacjach-na-rzecz-bezpieczenstwa-publicznego.pdf> (accessed: 6. 04. 2022).

²⁹ <http://www.anti-drone.pl/informacje/rozwiązania> (dostęp: 7. 04. 2022).

e) control interference - the detailed implementation of this mode of operation is an expression of the individual company's approach. Emission of high - power signals in the operating band of the control is noise that "covers" the proper signals. The drone does not receive commands from the control panel causing its reaction, which is foreseen by the drone manufacturer in such a case. The effects can be various, including: returning the drone to the starting point, immediately starting the landing process, causing it to fall and crash.

Operators and managers of critical infrastructure are quite active in developing systems which can reduce the likelihood of attacks on protected objects and systems. Examples include the interest in various anti-drone systems, which were described in a very synthetic way in the previous section. Some of these systems operate in several locations.

Undeniably, with the further development of remote UAV technology, the countermeasure system will evolve to meet the requirements of providing an adequate level of security in the airspace.

The first tool to prevent the misuse of drones are the so-called passive countermeasures (strictly technical), the enforcement of which is the responsibility of the state and relevant institutions. They are based, among others, on classical radar systems for detection and monitoring. Passive countermeasures also include radio signal jammers and a system based on detecting UAVs due to the sound signals their propulsion systems emit.

The second type of remedy is called active remedies. They are the last layer of protection, used when other means have ultimately failed. Their purpose is to destroy or deactivate the drone in order to prevent it from continuing its flight. Deactivating the device by disrupting the GPS signal seems to be relatively the mildest way. The use of laser beams or guided missiles to destroy BSPs are means of immediate destruction, more rigorous in their operation. Such methods have already been tested and are available. Today, advanced forms of security are being sought as a primary or complementary tool for safety, prevention, protection and management. The aim is to achieve a state of non-threat, providing certainty and guaranteeing the maintenance of a sense of security. This sense of security, whatever its level and scope, has a significant impact on the complexity of issues in many spheres of our lives and is constantly evolving, especially in terms of subject matter. The need for insecurity has given impetus to the implementation of intelligent security systems for monitoring, surveillance, signaling and patrolling.

Drones for the benefit of public safety can be successfully used, for example, to monitor and control places that are difficult to access or dangerous; to monitor the technical condition of a facility in the context of early identification of a threat; to verify an alarm; to patrol from the air; to control the quantity of goods in case of suspected theft. On the other hand, we encounter unauthorised attempts to use UAVs in the context of invasion of privacy, smuggling, spying or terrorist actions against public objects or critical infrastructure. Each such unauthorised action is aimed at acquiring information about a given target, recognising an object for the purpose of robbery, gaining knowledge about the business model or collecting data on the company's development, which is especially true of manufacturing plants. The list of objects at risk of unwanted drone actions is getting longer. This is due to the growing awareness on the part of those managing the sites in question. Entrepreneurs of large production plants, logistics and forwarding companies, critical infrastructure facilities, governmental, recreational and sports facilities and private ones are noticing the problem of wide-ranging surveillance by those making unauthorised flights over their facilities. The above activities are the basis for manufacturers to create more and more modern devices or systems to identify and neutralise drones in a threatening situation.

SUMMARY

In conclusion, it is possible to point to a number of recommendations that should be considered when creating and using anti-drone systems designed to protect the critical infrastructure of the state. The recommendations boil down to the main postulate that it is necessary to introduce effective anti-drone systems 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 for CI protection. The introduction of effective anti-drone systems will allow for effective management of the security of the state's critical infrastructure. In addition, specific recommendations may be indicated, namely:

1. The most vulnerable elements of critical infrastructure with high drone threat potential are: energy supply systems, raw materials and fuels; communication systems; ICT network systems, systems of production, storage, storage and use of chemical and radioactive substances, including pipelines of hazardous substances and rescue systems. The logical response of an organisation to a disruption is to build a homeostasis mechanism based on

monitoring threats, neutralising them, and when this fails, restoring the state before the disruption, and until then providing forms of substitute action. Such behaviour is an expression of a rational response to an unavoidable risk. Detailed analysis of the mechanism of such behaviour leads to the definition of criteria for rational risk assessment and model attitudes of response, appropriate to the magnitude of the potential impact of the risk.

2. All the elements indicated above have an impact on security management, which relies heavily on ensuring business continuity. In this sense, ensuring business continuity is the subject of strategic management, expressing the overarching objective of organisational agility and taking primacy in the area of operational risk management.

3. Business continuity is extremely important, understood as an organisational behaviour, creating the ability of the organisation to respond effectively in a situation of disruption resulting from the specific interaction of manifestations of threat with the vulnerability of the internal organisation, infrastructure or resources. In this sense, ensuring business continuity is the subject of operational management and is the last link in operational risk management.

REFERENCES LIST

LITERATURE

- Holliday B., *Drones: The Complete Collection*, CreateSpace Independent Publishing Platform, 2017.
- Polkowski P., Bezzałogowe statki powietrzne unmanned aerial vehicles, „Rocznik Bezpieczeństwa Międzynarodowego” 2016, 10(1).
- Tuśnio N., Nowak A., Tuśnio J, Wolny P., Bezzałogowe statki powietrzne w działaniach Państwowej Straży Pożarnej – propozycja dedykowana Państwowej Straży Pożarnej, Zeszyty Naukowe SGSP 2016, 58, tom 1/2.
- Zawiła – Niedźwiecki J., Ciągłość działania organizacji, „Prace Naukowe Politechniki Warszawskiej. Organizacja i Zarządzanie Przemysłem”, 2008/z. 20 / 3–07.
- Fellner R., Mańka A., Kursy operatorów bezzałogowych statków powietrznych - "Prawo jazdy na drony (UAV)", www.bsp.2ap.pl, www.ktl.polsl.pl.
- Holliday B., *Drones: The Complete Collection*, CreateSpace Independent Publishing Platform, 2017.
- Drony w służbie społeczeństwa, „Innowacje techniczne”, 2016 <https://iq.intel.pl/drony-w-sluzbie-spoleszczenstwa>.
- <https://rcb.gov.pl/narodowy-program-ochrony-infrastruktury-krytycznej-przyjety-przez-rade-ministrow-2>.
- <http://www.anti-drone.pl/informacje/rozwiązania>.
- <https://www.cnbop.pl/wydawnictwa/ksiazki/978-83-948534-6-4/wykorzystanie-bpp-w-operacjach-na-rzecz-bezpieczenstwa-publicznego.pdf>.
- <https://bzbuas.com/blog/aktualnosci/co-to-jest-uav-uas-bez زالogowe-statki-powietrzne/>.
- WEF_The_Global_Risks_Report_2021.pdf, WEF_The_Global_Risks_Report_2022.pdf.

SOURCES

Ustawa z dnia 27 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz. U. 2007 nr 89 poz. 590.

Rozporządzenie (UE) 2018/1139 w sprawie wspólnych zasad w dziedzinie lotnictwa cywilnego i utworzenia Agencji Unii Europejskiej ds. Bezpieczeństwa Lotniczego.



Copyright (c) 2022 Grzegorz PIETREK



This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.