Grzegorz Pietrek
Siedlce University of Natural Sciences and Humanities
grzegorz.pietrek@uph.edu.pl
ORCID ID: 0000-0003-2660-8025

JOURNAL OF MODERN SCIENCE
TOM 2/49/2022
www.jomswsge.com
DOI: https://doi.org/10.13166/jms/155797

THREATS TO CRITICAL INFRASTRUCTURE. THE CASE OF UNMANNED AERIAL VEHICLES

Summary

The problem area noted by the author of this paper is the existence of threats to the critical infrastructure of the state, especially from rapidly developing "drone" technology. The main objective of the research was the following: assessment of potential threat to the state's critical infrastructure from unmanned aerial vehicles. To achieve the outlined objective, the author mainly used the following theoretical methods: analysis of the literature on the subject, analysis of legal acts, synthesis, analysis (inductive and deductive), abstraction, comparison, and inference. Inference was carried out based on SWOT analysis, a method from the strategic management group. The main conclusions that emerged from the research process boil down to drones being a new threat to critical infrastructure; fully effective warning and elimination systems having not yet emerged; considerable emphasis needing to be placed on infrastructure owners and operators needing to take this threat into account.

Keywords: *critical infrastructure, security management, strategic management, unmanned aerial vehicles*

Introduction

The development of various types of hazards is an obvious consequence of an increase in technological advancement. There are diverse threats to people, property and the environment. It is possible to find in this thicket of different definitions, criteria and concepts also those that relate to the security of critical infrastructure. After analyzing the available literature and studying the current legislation, it can be concluded that one of the threats that has emerged relatively recently and seems to be relevant and "developing" is the threat from "Unmanned Aerial Vehicles", commonly known as drones. This article is intended to indicate and highlight a new type of threat to the State's Critical Infrastructure (CI). For the purpose of this paper, a specific research objective was defined, i.e., to assess the potential threat to the state's critical infrastructure from unmanned aerial vehicles. In the next stage, the research problem was defined as follows: What is the scale of threats to the state's critical infrastructure from unmanned aerial vehicles?

The following thesis was adopted as the main research hypothesis: the scale of threats to the state's critical infrastructure from unmanned aerial vehicles is significant and will grow in the long-term. Realizing the above-mentioned research objective, a variety of research methods were used: theoretical methods – analysis of the literature on the subject, analysis of legal acts, synthesis, analysis (inductive and deductive), abstraction, comparison, and inference. Inference was carried out based on SWOT analysis, a method from the strategic management group.

Topics connected with state's critical infrastructure

In the Republic of Poland, critical infrastructure is included in eleven systems that are crucial to the security of the state and its citizens and serve to ensure the smooth functioning of public administration bodies, as well as institutions and businesses. Most of the adopted definitions are derived from the content of current legal acts, which precisely define measures of great

importance for the smooth functioning of both society and the economy (Tyburska, 2016, p. 233).

In the Polish legal system, the issue of critical infrastructure is presented in the Act of April 27, 2007, on crisis management, in which Article 3 (2) specifies that *critical infrastructure should be understood as systems and their functionally related objects, including buildings, equipment, installations, services that are key to the security of the state and its citizens and that serve to ensure the efficient functioning of public administration bodies, as well as institutions and entrepreneurs* (Ustawa z dnia 27 kwietnia 2007 r. o zarządzaniu kryzysowym, art. 3, ust. 2).

According to the content of this article, it can be assumed that permanently and invariably among the elements that make up critical infrastructure are the systems of: energy supply, energy resources and fuels; communications; information and communication networks; finances; food supply; water supply; health care; transportation; rescue services; ensuring the continuity of public administration; production, storage, storage and use of chemical and radioactive substances, including pipelines of hazardous substances (Ustawa z dnia 27 kwietnia 2007 r. o zarządzaniu kryzysowym, art. 3, ust. 2).

An unmanned aerial vehicle, in its simplest definition, is a machine that does not require a crew present on board to fly, does not have the ability to carry passengers and is piloted remotely or performs flight autonomously. In fact, the aircraft itself requires additional resources and equipment to operate. These devices communicate with each other and enable the aircraft to perform its assigned task.

UAS (or Unmanned Aerial System), on the other hand, consists of the following components. (https://bzbuas.com/blog/aktualnosci/co-to-jest-uav-uas-bezzalogowe-statki-powietrzne/ [access: June 7, 2022]):

- UAV – Unmanned Aerial Vehicle;
- ground control station (GCS), operated by the operator;
- communication system between the control station and vehicle in the air;
- an interchangeable payload, used depending on the nature of the mission being performed;
- software for processing the data collected;
- support equipment, for transporting and operating the entire system.

The word "drone" is the same as the technical term Unmanned Aerial Vehicle (or UAV). It is the most common term in media, the most often used term in journalism, as well as by hobbyists and amateurs. It is erroneously assigned to anything that flies and is remotely controlled. For example, a separate group are RC models, colloquially called "racers" by their admirers.

The name drone itself is derived from the English word *drone*, which is a stingless male bee. The field of drones –multi-rotor drones, which have gained the most popularity in recent years— make a distinctive sound when flying that is produced by their rapidly spinning propellers, similar to flying drone bees. We can divide Unmanned Aerial Vehicles into several categories, depending on their construction and propulsion systems.

Multirotors – Their movement is thanks to the lifting force produced by several propellers (rotors) placed symmetrically around the perimeter of the drone. They are very maneuverable and easy to operate, learning to control them takes a very short time. The advantage of this type of construction is the possibility of vertical takeoff and landing, which makes it possible to carry out operations in places where the use of other techniques is difficult or impossible. The main disadvantage of multi-rotors is the relatively short flight time. For this reason, this type of drone is used most often when surveying point objects or objects with a small area (heaps, pits, structures).

Airframes – These most resemble classic airplanes. Propulsion is provided by propellers on the wings or beak, and control is through flaps on the wings and tail. They take off from the hand or a special launcher. They are characterized by very long flight times (even several hours) and are used to scan large areas, often linear in nature (agricultural fields, roads, gas pipelines, power lines). Airframes are more complicated to operate than multirotors. Most commercially available platforms only allow automatic flight – the user has no way to take control. A key moment is the landing approach. Determining the correct approach path requires experience and mistakes often result in crashing the aircraft.

Helicopters – helicopters resemble classic helicopters. Propulsion and control are provided by two rotors – a carrier and a tail rotor. Helicopters are much heavier to operate than other types of drones. Servicing and simply preparing the drone for flight is more difficult. The main reason for this is the complicated head mechanism that controls the angle of the carrier rotor

blades. However, helicopters can stay in the air longer than multi-rotors, often up to two hours. They can also, similarly to multi-rotors, perform vertical takeoffs and landings.

Hybrids – Also called vertical takeoff airframes, are a combination of certain features from airframes and multi-rotors. They are easy to control, can take off in difficult terrain, and stay in the air for up to several hours.

At the heart of every drone is an autopilot, which controls the machine, stabilizes its flight and allows it to perform autonomous flights. The drone itself is just a tool; it still needs a component that gives it a useful value, such as a camera or sensor. In addition to flights purely for amusement, each craft needs a device that receives and processes the signal reaching it from the object under study. The most common types of such cameras and sensors are:

- LIDAR – Light Detection and Ranging. This works similarly to radar or sonar, but instead of microwaves or sound waves, it uses reflected visible light from a laser. Using a laser, short pulses of light of a specific wavelength are sent out. The reflected light is recorded by a photodiode or CCD camera, for example. By studying the intensity of the scattered light pulse, numerical models of the terrain are created, including coverage, such as roads, high-voltage lines, buildings, trees, etc.
- RGB camera – from Red, Green, Blue, meaning the colors red, green and blue – the three components in the RGB color model (hence the name). It's actually an ordinary camera, capturing the spectrum of visible light. With an RGB camera, it is possible to create maps of an area while maintaining accurate color reproduction – exactly as a human would see it.
- Multispectral and Hyperspectral Sensor – Multispectral, super and hyperspectral sensors are generalizations of the RGB camera. In addition to the visible light spectrum (RGB), they are capable of recording other spectra, such as various ranges of infrared or microwaves. In simple terms, macro-components absorb solar radiation and distort it (absorb part of it) then give back a wave of a different length, a multi-, hyperspectral sensor accurately measures the intensity of waves in different lengths, so we know the exact composition of the macro-components. Based on the analysis of reflected infrared waves, it is possible, for

example, to visualize the NDVI index for analyzing plant vegetation, determine soil moisture or the course of underground pipelines. This is not possible with an ordinary RGB camera

Very broadly speaking, unmanned aerial vehicles can be used wherever collecting data on space from the ground is difficult, time-consuming, dangerous or impossible:

- digital orthophotos;
- thermal imaging measurements;
- 3D models of objects, cities and buildings;
- crop monitoring, estimation of hunting damage;
- monitoring of forest areas;
- monitoring of state borders;
- handling of mass events;
- rescue operations, Search and Rescue;
- disaster area survey;
- military missions;
- filming and occasional photography.

As indicated earlier, unmanned aircraft are equipped with various types of effectors (radar sensors, optoelectronic heads, spectrum analyzers, acoustic sensors), which can be used for observation, transmission of information and positioning of an enemy. These devices can also be used as simple air carriers to carry explosives, weapons, poisonous agents, or smuggled drugs across national borders. These devices, in contact with another participant, aircraft or cars, poses a serious threat to airports, highways other critical infrastructure components, etc. Despite flight bans, there have been notorious cases of violations. A drone is a flying device that moves at low speeds and low altitudes, making them difficult to detect. In addition, they still have a very small reflective surface, as a result of which they are very difficult to recognize by radar. It is also difficult to determine the devices owner or pilot. This is because it is controlled from a distance using, for example, an LTE Internet network. This can be done from a laptop from anywhere in the world. With the development of technology, regulations are being changed with regard to

aviation law, which today prohibits unmanned control unless its weight does not exceed 0.6 kg. Unmanned aircraft can be used in positive ways, such as surveying or taking aerial photographs. However, there is a danger that the control signal may be intercepted and the unmanned aircraft could change hands.

Today's drones pose a challenge critical infrastructure. Drones are very quiet, cannot be heard and are difficult to see, 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 possible to fly with impunity through drones.

Probability of interruption of CI operations

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 UAVs on the continuity of the state's critical infrastructure through the prism of the realization of the national interest. Nowadays, the security of critical infrastructure not only forms the basis of the state's operation, but is even a sine qua non for its functional existence. Accordingly, public administration is taking measures to protect as effectively as possible the services without which it is difficult to imagine a modern state. One of the key elements of these measures is undoubtedly the creation of an appropriate regulatory environment. Critical infrastructure legislation faces three main challenges (Zawiła-Niedźwiecki J., (2008) *Ciągłość działania organizacji*, p. 32):

- Predicting the type and intensity of a potential crisis that could negatively affect critical infrastructure;
- Providing appropriate tools to respond to a crisis;
- maintaining the proportionality of the tools created, by maximizing the protection of public safety and minimizing the negative impact on individual freedoms.

Organizations function in a rapidly changing environment, under the constant influence of strong pressures related primarily to the need to constantly reduce operating costs and protect themselves from possible disruptions. The realization of these tasks through the possession of modern technical infrastructure, increasing the qualifications of employees, compliance with standards and legal acts and similar constant competition with other entities has caused the emergence of threats to the state's functioning. As a result, more and more is being heard about business continuity management, which aims to identify the potential impact of disruptions on the organization and create conditions for building resilience in them and the ability to respond effectively in terms of protecting the key interests of owners, the reputation and brand of the organization, as well as the values achieved in its past activities, i.e., (Zawiła-Niedźwiecki J., (2008) *Ciągłość działania organizacji*, p. 33):

- guarantee the continuation of business processes;
- minimize the threat of loss of critical assets;
- minimize the loss of time and energy for restoring proper business processes or recovering lost resources;
- manage the quality and image of the company;
- avoid legal consequences resulting from failure to comply with applicable regulations.

Acquiring full knowledge of all threats is virtually impossible. Mainly because the variety of phenomena that pose a threat to the achievement of the company's intended goals is enormous. These dangers are born in various organizational-legal, economic-financial, technical-technological and other conditions. This means the emergence of new risks and the metamorphosis of existing ones. The logical response of an organization to disruptions is to build a mechanism of homeostasis based on monitoring threats, neutralizing them, and when this fails, restoring the state before the disruption, and until then providing forms of substitute action. Such conduct is an expression of a rational response to unavoidable risks (Rynkiewicz W. (2016) *Infrastruktura krytyczna*, p. 151).

Detailed analysis of the mechanism of such behavior leads to the determination of criteria for rational risk assessment and model response

attitudes appropriate to the magnitude of potential risk impact. In particular, the rationality of response is based on the assessment of risk intensity factors, i.e., the strength of its impact (especially potential damage) and the frequency of impact (Zawiła-Niedźwiecki J., (2008) *Ciągłość działania organizacji*, p. 34).

Business continuity, first of all, is a postulate of excellence of the system of operation, which is any organization, and therefore any economic or administrative entity. In this sense, ensuring business continuity is the subject of strategic management, that expresses the primary goal of organizational agility and takes primacy in the area of operational risk management.

Secondly, business continuity is understood as organizational conduct that creates the organization's ability to respond effectively in a situation of disruption that results from the peculiar interaction of the manifestation of a threat with the vulnerability of the internal organization, infrastructure or resources. In this sense, ensuring business continuity is the subject of operational management and is the last link of operational risk management.

In general, business continuity is the ability of an organization to respond to disruptions in the conditions of normal operations in such a way that, where possible, these normal conditions are quickly restored, and where this is not possible, to move to a planned method of substitute task performance. Business continuity is thus takes into account the organization's tasks and the processes used to carry out these tasks, the factors that can disrupt these processes and the forms of vulnerability of the organization that constitute its vulnerability to disruption.

Assuring business continuity includes (Zawiła-Niedźwiecki J., (2008) *Ciągłość działania organizacji*, p. 39):

- the organization's response mechanism to disruptions;
- the process of developing the aforementioned disruption response capability mechanism (as a process supporting – in the sense of process analysis – the core business of the organization);
- the process of managing the capability of ongoing business continuity and its continuous improvement.

The mechanism for responding to disruption consists of (Zawiła-Niedźwiecki J., (2008) *Ciągłość działania organizacji*, p. 39):

- an organizational structure dedicated to the task of ensuring continuity, forming a coherent whole with the overall organizational structure;
- formal organizational regulations defining the relationships in the organizational structure related to the task of ensuring continuity;
- established practice (possibly written down) for dealing with situations where a response to a disruption is required.

First of all, it should be emphasized that responding to disruptions by ensuring business continuity should be understood not only as directly handling disruptions, but also as a preventive activity, related to the analysis of threats and vulnerabilities and the search for methods and solutions to prevent disruptions. In this sense, business continuity and security efforts are intertwined. From a business continuity perspective, security solutions provide prevention against threats, while from a security perspective, business continuity solutions provide additional security. This justifies the concept of managing both issues together, and likewise quality management (Zawiła-Niedźwiecki J., (2008) *Ciągłość działania organizacji*, p. 39).

The effect of dangers caused by the use of unmanned aerial vehicles

The global market has seen a tremendous increase in the popularity and application of drones (unmanned aerial vehicles), from children's toys to drones that inspect objects or take landscape photos, to those that even provide military solutions. Despite their many useful applications, it's not difficult to imagine drones also being used in undesirable activities such as invasion of privacy, terrorism, spying or smuggling. They can be used to peep at people, eavesdrop on politicians or businessmen, plan robberies of wealthy people or even carry out attacks with sharp weapons or explosives on selected people or objects. In the public sphere, they can pose a terrorist threat (a drone can carry an average payload of several kilograms) to public facilities and critical

infrastructure (power plants, airports, ports, refineries, etc.). They can also be used to smuggle drugs or weapons across borders, threaten military facilities or be used for espionage purposes.

An unmanned system can reach a considerable degree of complexity. As it grows, the number of potential attack vectors increases. It appears that an increasing proportion of critical infrastructure threats related to information systems can be generated by "drones" used to protect that infrastructure. Among the attacks that currently seem most viable are the following (https://cyberlaw.pl/drony/bezpieczenstwo-dronow/ [access: June 6, 2022]):

- Direct attempts to send malicious commands to the BSP;
  - » interfering with communications with the BSP;
  - » eavesdropping on unencrypted communications with the BSP;
  - » attempting to infect one part of the system with malware.

In the case where the communication protocol between the drone and the operator (GCS – ground control station) is known to the attacker and where the protocol does not implement sender authentication mechanisms, the attacker would be able to directly send a command to the BSP, which could be executed.

Another threat is the interference of communications by an attacker, in an extreme situation (lack of implemented security features) which could lead to the platform crashing. Given that most BSP applications involve aerial photography, if a video signal is transmitted to the operator in unencrypted form, it could be intercepted by an attacker. Finally, due to the frequent use of PCs and mobile devices in the form of a GCS, an attacker could infect the device with malware. An attack that is more difficult to carry out is so-called GPS spoofing, an action that involves broadcasting a GPS signal crafted in the vicinity of the drone in such a way as to provoke the movement of the BSP in the desired direction (https://cyberlaw.pl/drony/bezpieczenstwo-dronow/ [access: June 6, 2022]).

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

This is just the beginning of the "drone war." Attacks organized directly by and involving humans will become increasingly rare as they use technology

and science for a variety of purposes both positive and destructive to world order and peace.

Unmanned aerial vehicles, commonly known as drones, are piloted from a command center by a trained operator or have specific goals coded for them to achieve (they are fully autonomous). Thanks to the fact that they are guided remotely, there is no loss of in human lives, for example, after such a drone is shot down.

Potential terrorists who perpetrate attacks on CI facilities are very likely to use very light or lightweight drones. They are available almost anywhere and without much trouble. They also present almost no problems with operation, and their price is low enough that even their destruction in the failure of a potential terrorist act is not felt in any significant way. While lightweight drones won't carry heavy payloads, even a small amount of anthrax bacteria is capable of killing many people. It is also possible to attach a digital camera to the drone, which will allow 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 chemical. The introduction of dangerous viruses and bacteria into groundwater or large bodies of water threatens large numbers of the population with loss of health or even life. A drone can carry a hazardous substance (e.g., viruses or bacteria) over a larger concentration of people (e.g., during 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 tank of petroleum at a fuel base. Unnoticed, a small unmanned flying object can paralyze the traffic of an airport or endanger the health and lives of people by planting a payload in an oil port, which additionally carries huge financial losses.

Unmanned aerial vehicles equipped with good optics and image recording (on an internal disk or with the ability to transmit the image directly to the operator) could be used by potential terrorists to draw a location map of the point which an attack would be most impactful and cause the most damage. Such an attack could occur on a facility in the oil and energy industry. For example, during a terrorist attack with a drone on the energy sector, there could be a so-called blackout, i.e., a blackout of the power grid over a large area (http://www.anti-drone.pl/informacje/rozwiazania [access: June 7, 2022]).

Conclusions

After the study, there are several recommendations that should be considered in efforts to effectively protect the country's critical infrastructure. The recommendations mainly boil down to the main postulate that it is necessary to introduce effective anti-drone systems very widely. Such systems have already been 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 most vulnerable with high potential for drone threats are such critical infrastructure elements as energy, energy resources and fuel supply systems; communications systems; ICT network systems, systems for the production, storage, warehousing and use of chemical and radioactive substances, including hazardous substance pipelines, and emergency response systems. The logical response of an organization to a disruption is to build a homeostasis mechanism based on monitoring threats, neutralizing them, and when this fails, restoring the state before the disruption, and until then providing forms of replacement action. Such conduct is an expression of a rational response to unavoidable risks. Detailed analysis of the mechanism of such conduct leads to the determination of criteria for rational risk assessment and model response attitudes appropriate to the magnitude of the potential impact of the risk. All the elements described above have an impact on security management, which is largely based on ensuring business continuity. In this sense, ensuring business continuity is the subject of strategic management, expressing the primary goal of organizational agility and taking primacy in operational risk management. Of utmost importance is business continuity understood as organizational conduct, creating the ability of the organization to respond effectively in a situation of disruption resulting from the peculiar interaction of the manifestation of a threat with the vulnerability of the internal organization, infrastructure or resources. In this sense, ensuring business continuity is the subject of operational management and is the last link of operational risk management.

References

Panasiuk A., Sierański S., (2017) *Bezpieczeństwo państwa i obywateli. Ochrona obiektów infrastruktury krytycznej*. [w:] „Kontrola Państwowa" Nr 1, styczeń – luty 2017, s. 781 – 782.

Rynkiewicz W. (2016) *Infrastruktura krytyczna*, [w:] Ścibiorek Z., Zamiar Z. (red.), *Teoretyczne i metodologiczne podstawy problemów z zakresu bezpieczeństwa*, Wydawnictwo Adam Marszałek, Toruń, s. 151.

Tyburska A. (2016) *Zarządzanie kryzysowe wobec zagrożenia terroryzmem* [w:] *Bezpieczeństwo państwa a zagrożenie terroryzmem*, t 2, Jałoszyński K., Aleksandrowicz T., Wiciak T., (red.), Wydawnictwo WSPol., Szczytno, s. 233.

Wiercińska – Krużewska A., Gajek P., *Prawne uwarunkowania ochrony infrastruktury krytycznej* [w:] *Bezpieczeństwo infrastruktury krytycznej wymiar teleinformatyczny*, https://ik.org.pl/wp-content/uploads/bezpieczenstwo-infrastruktury-krytycznej--wymiar-teleinformatyczny_net.pdf [dostęp: 5.06.2022].

Zawiła-Niedźwiecki J., (2008) *Ciągłość działania organizacji*, „Prace Naukowe Politechniki Warszawskiej. Organizacja i Zarządzanie Przemysłem", 2008/z. 20 / 3 – 107, s. 32 – 33.

Żuber M., (2014) *Infrastruktura krytyczna państwa jako obszaru potencjalnego oddziaływania terrorystycznego*, „Rocznik Bezpieczeństwa Międzynarodowego", nr 2, s. 179.

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

https://cyberlaw.pl/drony/bezpieczenstwo-dronow/ [access: June 6, 2022.]

http://www.anti-drone.pl/informacje/rozwiazania [access: June 7, 2022].

https://bzbuas.com/blog/aktualnosci/co-to-jest-uav-uas-bezzalogowe-statki-powietrzne/ [access June 7, 2022].

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