POLISH
ASSOCIATION
FOR NATIONAL
SECURITY

SECURITY OF CRITICAL INFRASTRUCTURE AGAINST THREATS FROM UNMANNED PLATFORMS

Raport PTBN
volume II (2021)

ISSN 2720-037X

National Freedom Institute
Centre for Civil Society Development

Civil Society Organisations Development Programme for 2018-2030
CSODev

The Raport PTBN, Volume II (2021): „Security of infrastructure critical to threats from unmanned platforms" (ISSN 2720-037X) was developed by members of the PTBN Problem Analysis Team composed of:
Jędrzej Łukasiewicz PhD
Michał Piekarski PhD
Maciej Kluczyński

The content of the Raport PTBN, Volume II (2021) includes only the private views of the authors and they cannot be identified with institutions whose authors are employees.
Raport PTBN, Volume II (2021): „Security of critical infrastructure in the face of threats from unmanned platforms" was closed on September 1, 2021.
The online version of the Raport PTBN, Volume II (2021) is its original version.
The online version of the journal is available on the www.PTBN.onlinewebside.

Polish Association for National Security
(KRS 0000583118)
ul. Lotników 91/13, 44-100 Gliwice
e-mail: zarzad@ptbn.online
www.PTBN.onLine

https://twitter.com/PTBNonLine
https://www.facebook.com/polskie.towarzystwo.bezpieczenstwa.narodowego/

Jędrzej Łukasiewicz PhD
Michał Piekarski PhD
Maciej Kluczyński

SECURITY OF CRITICAL INFRASTRUCTURE AGAINST THREATS FROM UNMANNED PLATFORMS

PTBN Polskie Towarzystwo Bezpieczeństwa Narodowego

Gliwice • 2021

Table of contests

INTRODUCTION /**5**

1. Identifying unmanned platforms as a source of threats to critical infrastructure facilities /**7**

2. Methods of detection of unmanned aerial vehicles /**13**

3. The neutralization methods of unmanned aerial vehicles /**15**

4. European and national aviation regulations and flight rules /**18**

5. Methods of protecting critical infrastructure against threats from unmanned aerial vehicles /**22**

6. Conclusions /**30**

INTRODUCTION

Due to the technological development of unmanned platforms and other areas in which they can be used, they should also be viewed as a potential threat to systems and their functionally related objects, including buildings, devices, installations, services essential for the security of the state and its citizens and to ensure the efficient functioning of public administration, as well as institutions and entrepreneurs, in short, the critical infrastructure (IK)[1].

We focus in the report on the unmanned aerial vehicles, because the vast majority of the critical infrastructure is onshore and they can relatively easily overcome the commonly used ground-based physical protection systems, and in relation to unmanned surface and submarine platforms as well as unmanned land platforms, they are more universal. Thus, they currently pose a potentially greater threat to the state's critical infrastructure.

As part of the unmanned aerial vehicles (UAV) we can distinguish the following types of platforms: unmanned aerial vehicles (A type), unmanned multirotors (MR type) and unmanned helicopters (H type). Each of the aforementioned UAV types is characterized by different properties that determine the way the platform is used – to be widely presented in the further part of the Report.

The authors of the Report assumed that the study focuses on UAVs with a typically civilian use, i.e. for non-military purposes, which, however, are part of terrorist activities[2] and sabotage against CI facilities. It should be mentioned, however, that there are also military UAVs used by state entities.

[1] The Act of April 26, 2007 on crisis management, Journal of Laws 2007, no.89, item. 590 as amended.

[2] More about terrorist threats in: *Terrorist threats and the anti-terrorist system in the Republic of Poland,* Raport PTBN, Volume 1 (2020).

The Report also uses other terms related to unmanned aerial vehicles interchangeably, i.e. drones, unmanned aerial vehicles and unmanned platforms.

The authors of the Report would like to emphasize that in the long term, taking into account the plans for the dynamic development of strategic energy infrastructure within Polish maritime areas, attention should be paid to the threats posed by unmanned underwater and surface vehicles – both civil and military. The threats especially to sea ports, LNG reloading and regasification terminal in Świnoujście, oil terminal in Gdańsk, drilling platforms in the Baltic Sea, or planned offshore wind farms and FSRU LNG terminal (*Floating Storage and Regasification Unit*), as well as submarine cable lines, submarine oil and gas pipelines, and submarine telecommunications cables. This subject will be presented in further PTBN studies.

1. Identifying unmanned platforms as a source of threats to critical infrastructure facilities

An unmanned aerial vehicle (UAV) can be used as a kinetic or non-kinetic attack tool against critical infrastructure (CI) facilities and devices. From the point of view of the perpetrators of threats, the use of this type of flying devices has several important conditions, potentially increasing the effectiveness of an attack. Considering the basic features of unmanned aerial vehicles, i.e. the ability to fly, no crew on board, control systems allowing for a remote-controlled flight or according to a given scenario, including autonomous flight based on artificial intelligence[3], as well as in the case of most structures, the possibility of taking off and landing in off-road terrain, i.e. not requiring special infrastructure, the following factors can be indicated:

Mobility – due to its flight capability, the UAV is able to avoid artificial and existing natural terrain obstacles. In the case of CI facilities, this means the possibility of flying over the fence or other obstacle and avoiding ground, technical and personal security measures (gates, fencing, peripheral and perimeter zones, control posts, patrols). It is also possible to access hardly accessible facilities, such as those located at sea or in heavily forested zones.

Maneuverability – UAV, especially remotely controlled, can perform the flight (and in the case of rotorcraft even hover) in the indicated place, which allows it to be precisely directed at the element of the IK facility selected by the controlling flight.

[3] See https://www.thetimes.co.uk/article/killer-drones-used-ai-to-hunt-down-enemy-fighters-in-libyas-civil-war-2whlckdbm; https://www.newscientist.com/article/2282656-israel-used-worlds-first-ai-guided-combat-drone-swarm-in-gaza-attacks/.

Load carrying capacity – most UAVs can carry loads of different types and weights, e.g. weapons or improvised explosives.

Low detection level – Depending on the technical parameters (optical, acoustic, radar signature), UAV may not be detected by persons responsible for the protection of the CI facility or detected too late for effective counteraction. The low level of detection is also due to the possibility of flying at a very low altitude and between ground objects.

Discretion – UAVs, due to the relatively small dimensions of most structures, compared to manned aircraft, can be stored and transported in a way that does not raise suspicions. In addition, the popularity of recreational application of commercial devices allows the perpetrators of attacks to hide their use under the guise of legal and harmless activity.

Limitation of risk – the use of UAV to attack the IK facility allows the perpetrator, thanks to remote control, to minimize the probability of detection and thus arrest, which occurs when trying to penetrate or physically enter the CI facility.

Cost reduction – UAVs, due to their features, can potentially reduce the cost of an attack, to recognize the security system from a distance that limits the probability of its detection, which should increase the effectiveness of the attack without the need to incur higher own costs, e.g. creating the appearance of allowing penetration into a protected object or acquisition to cooperate with people employed there (so-called insider threat).

The above general assumptions should be confronted with empirical experiences. The history of unmanned aerial vehicles is long and is associated with their early, experimental combat use. They are mainly used nowadays, for tasks defined as *Dull, Dangerous, Dirty,* in which the presence of the crew on board is not necessary due to the nature of the flight operation (e.g. long-term monitoring of a given area) and would involve an unacceptably high risk or exclude the presence of the crew at all, e.g. due to extensive air defense systems[4].

[4] *Dull Dirty and Dangerous,* Flight International, https://www.flightglobal.com/dull-dirty-and-dangerous/2390.article.

Threats to CI facilities from the air may occur in several forms, including: reconnaissance, message transmission (propaganda), carrying explosive devices, carrying weapons of mass destruction, using weapons mounted on UAVs[5].

The reconnaissance of the object is the least invasive of them. This can take place in particular by performing UAV flights equipped with a camera (including the one with the thermal or infrared option) taking photos or videos. It is also less likely, though possible, to conduct reconnaissance in another way, e.g. radio-electronic reconnaissance (ELINT) or even transferring sensors (microphones, cameras) to the site. The information obtained in this way may allow the assessment not only of the topography of the object, but also identification of potentially vulnerable places, setting a schedule the functioning of the facility (e.g. security, supplies, etc.). Though the effectiveness of the use of an unmanned platform depends on many factors, such as the pilot's training level, the correctness of the mission programming, weather, UAV design, as well as the selection of sensors for the attack scenario.

A special case of reconnaissance is the deliberate disclosure of the unmanned platform as a source of threat to the CI facility in order to observe the type and manner of operation of the potential detection system and the procedures in force at the facility. Information may then be collected on the timing and manner of response, including type and quantity forces and means used[6]. Due to the availability of UAVs equipped with cameras, that method of using the unmanned platform is possible for any potential attacker, regardless of the financial resources.

The use of unmanned platforms for propaganda purposes is also a non-kinetic activity. It is possible to imagine by a potential attacker a recording of the flight of the UAV over an IK facility, with the aim to publicize the identified gaps in the security system of a given protected facility or to evoke a sense of threat among the inhabitants of the local community[7].

Carrying explosive devices is one of the possibilities of a kinetic attack on the CI object. In such a scenario, the UAV carries an improvised or factory-prepared explosive device.

---

[5] Bunker R.J., *Terrorist And Insurgent Unmanned Aerial Vehicles: Use, Potentials, And Military Implications,* Strategic Studies, Institute and US Army, War College Press, August 2015.

[6] Rogoway T., *Adversary Drones Are Spying On The US And The Pentagon Acts Like They're UFOs,* The War Zone, https://www.thedrive.com/the-war-zone/40054/adversary-drones-are-spying-on-the-us-and-the-pentagon-acts-like-theyre-ufos.

[7] Piekarski M., Wojtasik K., *The Polish anti-terrorist system and the realities of the attacks of the second half of the 21st century,* Toruń 2020, pp. 191-195.

It can be mounted or attached to the UAV and be dropped during an attack or remain a part of its structure. In the latter case, the platform carrying the explosive device self-destructs – it is the so-called circulating loitering ammunition *kamikaze drone*). The use of an unmanned aerial vehicle as a carrier of weapons of mass destruction (e.g. chemical) may have a similar character.

Finally, other forms of using UAV are also possible, e.g. to harass people working in CI facilities, protecting them or intervening. Cases of such application of unmanned platforms against state officials, although not in the context of CI[8].

The unmanned aerial vehicles, due to their construction, can be used in air missions of various types. Therefore, each terrorist organization can use them in a convenient way and come up with an attack scenario that has not been seen so far, thus surprising the protection system used in a given CI facility, based on internal risk analysis.

Terrorist organizations have no problems with acquiring unmanned platforms and spare parts for them by making purchases on the Internet and, thanks to smuggling, using intermediaries, as ISIS did it by smuggling drones into Syria and Iraq[9].

Unmanned platforms can be relatively easily armed, but in the case of flying platforms, however the so-called maximum mass that can be lifted by a given platform is the factor limiting the mass of the explosive device. It is possible to see in the materials available on the Internet, platforms produced by one of the leading drone manufacturers, which were equipped by ISIS members with multifunctional grenades of their own production. It is possible to find in these materials also a non-factory quadrocopter multi-rotor, which was equipped with an anti-tank PG-7 grenade for the RPG-7[10]. The validated data on flight performance, attack precision and the effectiveness of the use of these platforms, are missing.

Both the factory-made and self-constructed UAVs are able carry heavy loads, however the load weight depends mainly on the correct selection of propellers, motors, batteries and the mechanical strength of the frame. The 600 Pro, produced by DJI Matrice

[8] See e.g. Tucker P., *A Criminal Gang Used a Drone Swarm To Obstruct an FBI Hostage Raid,* https://www.defenseone.com/technology/2018/05/criminal-gang-used-drone-swarm-obstruct-fbi-raid/147956/.

[9] Rassler D., *The Islamic State and Drones: Supply, Scale and Future Threats,* https://ctc.usma.edu/wp-content/uploads/2018/07/Islamic-State-and-Drones-Release-Version.pdf.

[10] *Islamic State's Multi-Role IEDs*, https://www.conflictarm.com/perspectives/multi-role-ieds/; Watson B., *The Drones of ISIS,* Defence One, https://www.defenseone.com/technology/2017/01/drones-isis/134542/.

can carry a load of up to 6 kg, with the flight time of 16 minutes[11]while the larger, agricultural Argas T10 can carry up to 10 kg of cargo for approx. 9 min. of flight at the maximum take-off mass[12].

The available data indicate that not only the above-described multirotor UAVs, but also airplane UAVs can be used to carry out a terrorist attack, e.g. as it happened in 2012 in the USA, when the perpetrator who intended to use a rebuilt large airplane models (F-4 and F-86) as an attack tool[13].

It is possible to attack with UAV almost any object, installation, device, and the consequences of the attack will depend on the energy released during the explosion carried by the explosive device through the platform.

Terrorist organizations can also use unmanned combat platforms, made available to them by countries using these organizations to achieve their political goals as part of their hybrid operations. The devices designed by specialists and built by the arms industry are used in such a case. Such platforms can be adapted for performing specific tasks depending on the nature of the conflict, the specificity of the attacked CI object and the expected consequences of the attack.

The unmanned platforms can be used in such scenarios by the ad hoc trained persons (terrorists, separatists) or their own personnel (intelligence services or special force). The unmanned aerial vehicles can be secretly separately transported to the territory of the attacked country or catapulted, for instance, from vessels remaining outside the territorial waters. For example, the Iran-sponsored Houthi movement in Yemen uses Qasef-1 type loitering ammunition, a variant of the Iranian Ababil system. The device is capable of carrying an explosive of 30-45 kg weight and has a range of up to 150 kilometers[14]. In turn, the smaller, and thus easier to transport, the Russian Lancet-3 carries a warhead of 1 kg for a distance of up to 40 kilometers[15]. A significant advantage of using military systems is that they are equipped with advanced observation and control systems that allow them to attack the target with the required precision. The warheads can be adjusted to the character of the attacked object, as a result of what

[11] https://www.drony.net/matrice-600-pro-dji.html.

[12] https://enterprise.dji-ars.pl/produkty/agras-t10/.

[13] https://www.altair.com.pl/news/view?news_id=8965&q.

[14] Mushin D., *Houthi use of drones delivers potent message in Yemen War,* https://www.iiss.org/blogs/analysis/2019/08/houthi-uav-strategy-in-yemen.

[15] https://zala-aero.com/en/production/bvs/zala-lancet-3/.

the explosion of even a small charge can cause losses greater than a homegrown explosive device carried by commercially available platforms. The recent attack on the m / t Mercer Street off the coast of Oman using Iranian combat UAVs, most likely of the Delta Wing type[16] is an example.

Unlike terrorist organizations, the actions of state entities are usually multi-directional. The use of weapons may be preceded by a long gathering of intelligence, also through the use of political, diplomatic or economic channels. The scale of the threat is illustrated by the attack on 14/15 September 2019 on two oil refineries in Saudi Arabia using 18 UAVs and seven cruise missiles[17].

The attack resulting from asymmetric actions, in the case of terrorist organizations, or hybrid actions, in the case of state entities, may be used for propaganda purposes and described as an act committed by a non-state actor, e.g. a separatist or terrorist organization. In such a situation, an attempt to direct the narrative in such a way as to create the impression that it is an element of an internal conflict or even a form of provocation takes place. Thus, it may delay or prevent the application of adequate measures in response to the arisen threat. It should be considered for this reason, a threat of specific importance.

[16] https://www.centcom.mil/Portals/6/PressReleases/MERCERSTREETATTACK06AUG2%20final.pdf.

[17] Niedbała M., *Od Półwyspu Arabskiego do Narwi. Attack on refineries and Polish anti-aircraft defense,* Nowa Technika Wojskowa 1/2020.

2. Methods of detection of unmanned aerial vehicles

The method of detection of unmanned aerial vehicles should be adapted to the properties and physical characteristics of a particular type of platform (plane, multirotor, helicopter). The most commonly used methods of UAV detection include:

a) **Radar detection.** It allows the detection of UAVs of various sizes and shapes, located at a great distance from the radar antenna, and allows you to track many flying platforms at the same time. The disadvantage of this type of detection method is the limited possibility of detecting a UAV flying at a low altitude. Each terrain obstacle, including trees, buildings, small architecture objects, as well as various topography, is a potential place where the detection of flying UAVs will be difficult or even impossible.

b) **Acoustic detection.** The method is based on the analysis of sound recorded with a set of microphones and selecting from the entire recorded spectrum of the acoustic signal those frequencies that correspond to the frequencies of sound emitted by engines and UAV propellers previously recorded. The use of this method is limited in many ways. First of all, attention should be paid to the fact that each UAV, regardless of its type, can have an engine with a different spectrum of the acoustic signal. UAVs can be powered by both electric and combustion engines. The combustion engines are noisy and thus easily detectable, require specialized service, are relatively expensive and due to the high level of noise emitted, their use is limited by regulations[18]. The electric engines are quiet and their hum is less audible as the speed of the propeller rotation is lower. Depending on the location of IK facilities, the sound emitted by the flying UAV may be drowned out by sounds emitted by various other sources. The sounds emitted by the engines of cars, public transport

[18] Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 *on UAS and third country UAS operators*, NS. OJ. UE L 152, 11.6.2019 r.

vehicles, noises coming from a nearby construction site, etc. make it difficult or even impossible to detect UAV with the use of microphones.

c) **Detection by infrared or visible image.** For this type of detection, cameras that record images in the infrared or visible spectrum of electromagnetic radiation are used. The cameras record an image that is analysed by computer programs that use artificial intelligence (AI) technology. Algorithms detect objects in the recorded image and compare them to the pattern. The pattern in this type of detection devices is obtained by recognizing the algorithm what a is the flying object of with the right temperature or shape, and what is another object, e.g. a bird. Teaching a detection device to detect the right objects is a time-consuming process and requires from a programmer to have access to a database of photos depicting various UAVs. The image analysis method, as one of detection methods, is strongly dependent on the weather conditions. Any atmospheric phenomena that reduce the quality of the recorded image is an obstacle in UAV detection. As well the UAV structures that do not take after the previously known platforms with their shape will not be detected by image analysis. It is worth mentioning here the attack on the nuclear power plant accomplished by the international non-governmental organization Greenpeace using a platform in the shape of a flying Superman[19].

d) **Detection by discovering an electromagnetic signal,** by means of which communication between the UAV performing the mission and the base station through which the pilot controls the flight of the UAV is carried out. Currently, in commonly produced UAV systems, communication between the aircraft and the base station can take place at the frequencies of 2.4 GHz, 5.8 GHz and rarely at 433 MHz. Such communication can be detected and the transmitter tracked by the triangulation method. The disadvantage of this method is its total uselessness in the case where the UAV is programmed before start and will perform its mission in the total autonomy mode without communicating with the base station.

UAV detection systems are built of devices that use all the above-described detection methods, but none of them guarantees the detection of flying UAVs. The attacks performed with the use of UAV systems described in the literature explicitly indicate that the effectiveness of UAV detection systems is narrow A potential attacker with a basic knowledge of the principles of operation of detection systems can easily build a UAV, the detection of which will become almost impossible, and thus will be able to achieve the planned target of the attack.

[19] https://www.reuters.com/article/uk-france-nuclear-greenpeace-idUKKBN1JT17G.

3. The neutralization methods of unmanned aerial vehicles

The variety of unmanned aerial vehicle structures and their comprehensive technical capabilities enable the attack to be conducted in a variety of scenarios, being low cost and requiring relatively little technical knowledge of the platform constructor, they make UAV an extremely dangerous weapon. That is the reason why the UAV neutralization systems must be efficient in all conditions and for each structure. The use of the anti-drone system is subject to prior detection of a flying UAV. The most commonly used methods of UAV neutralization include:

a) **Disruption or jamming of the satellite navigation system.** Most of the UAVs presently produced for civil purposes, which can be used in an attack on CI facilities in the EU, are equipped with a receiver of the American GPS system, Russian GLONASS or European Galileo. Satellite navigation systems make it possible to control the position of an aircraft in the course of a flight. Also, most of the currently produced UAVs are equipped with software that allows for programming program the route before takeoff. Such programming consists in indicating the geographical location of the target points (WayPoints) to which the UAV must reach, the altitude at which these points are located, and the advance speed of the UAV in the course of a flight. The UAV programmed in this way can perform the mission without maintaining radio communication (thus without pilot operation) with the base station. The UAV will fly its flight based on the readings from two detectors: a barometric sensor indicating the altitude under the atmospheric pressure measurement, which is equipped with the UAV computer, and the satellite receiver, which the platform is equipped with. The satellite signal reaching the ground is weakened by being absorbed by layers of the atmosphere. It is technically possible to interfere with the navigation signal from the satellites. The disturbance may be that a navigation signal is emitted from the earth's surface, but with a much higher power than that

emitted from the satellite. This means that the navigation receiver will read this false signal as being valid. The aircraft will get lost in the air and will not discover the target of the attack. The disruption of the satellite signal will cause wrong position indications in the navigation also of other platforms, including e.g. car navigation or mobile phones. Satellite signal interference is becoming a common practice in hostilities, so technologies are being designed to navigate without using satellites[20].

b) **Communication signal disturbance between base station and BSP.** UAV flying in the direct control mode by the pilot communicates with the base station using electromagnetic waves of different frequencies. As already mentioned, the electromagnetic waves normally used in communication are those with the frequency of 2.4 GHz, 5.8 GHz and 433 MHz. It is possible to disturb this communication with an external device and make the UAV non-operational.

c) **Damage to electronic components with an electromagnetic pulse emitter.** An impulse of high energy and proper frequency is emitted towards the UAV. The electronic semiconductor components of all UAV electronics, including the computer, engine speed control (ESC) elements, satellite navigation signal receiver, receiver for communication with the base station are sensitive to electromagnetic pulses and are damaged. The electromagnetic impulse emission systems can be effective for typical mass-market UAVs. However, it is possible to prepare UAVs in such a way that they are insensitive to the electromagnetic pulse. This is accomplished by positioning the aircraft electronic systems in the shielded trays. These reservoirs are usually made in multilayer technology so that impulses of different frequencies are shielded. UAVs with screens protecting against electromagnetic impulses are not commercially available.

d) **Mechanical damage or interception of flying UAV with a net** boosted from a launcher usually mounted on another UAV in flight. The fired net wraps around its propellers or other moving elements of the intruder, causing it to fall to the ground. The net can be equipped with a braking system – a parachute, which, after opening, will allow the captured UAV to fall at a low pace. Thus, the UAV is not broken, and its electronics, including, for example, elements that record flight logs, can be used in clarifying proceedings and be a source of evidence in criminal cases. The net system, while it appears to be very effective in some conditions, has

[20] https://defence24.pl/wiceprezes-grupy-wb-nasza-lacznosc-jest-odporna-na-zaklocenia-to-efekt-wnioskow-z-donbasu-skaner-defence24.

weaknesses. One of such disadvantages is the one-off shot. The net launcher has only one net at its disposal, which means that after shooting out the UAV it has to return to the ground to load a new net. In the case of an attack conducted with more than one drone, such a system seems to be highly inefficient.

e) **Damage to the UVA with laser light by lighting it.** The light-emitting laser device must be powered by a high-power source of electricity. Most likely, the laser as an anti-drone weapon may become a standard equipment for protected facilities in the future. Presently, prototypes of this weapon are undergoing tests in almost laboratory conditions. The obstacles to the more popular use of lasers in order to combat UAVs include, among others, the dependence of the effectiveness of these weapons on weather conditions and the relatively long (several seconds) time needed to ignite the flying platform. In the event of precipitation or in the case of limited air transparency (e.g. due to haze), the laser light is absorbed by the water molecules. The long emission time of the laser light is an obstacle in the case of attack attempts with the use of several aircraft. In order to be effective, the laser system would have to be equipped with a set of lasers so that each hit a different UAV. The rapidly developing technology for controlling swarms of drones in the air and under water seems to eliminate practically the use of lasers in cases other than an attack by a single UAV.

All the above-described methods lead to the fall of the flying UAV to the ground. Therefore, it is necessary to consider what the consequences of such a fall will be. For instance, in the event of a UAV dropping down while unloading a tanker with LPG in an internal port, a disaster comparable to the explosion in the port of Beirut in 2020 could occur. Situations of this type are not sufficiently described in national regulations, in which the responsibility for the potential consequences of the landing of a UVA by entities with appropriate powers is not defined in a transparent and unambiguous manner.

4. European and national aviation regulations and flight rules

Uniform rules governing the construction of UEV and flight rules are currently in force in the European Union[21]. These regulations allow national aviation authorities to establish the so-called drone geographic zones. The applicable law depends on the type of drone geographic zone. Presently, after the introduction of a uniform European law in December 2020, the Member States are in the period of adjusting their national regulations to the EU requirements. In accordance with these regulations, flights take place in three categories: open, special and certified. **Open category** is a low risk flight category. Flights in this category do not require approval for an operation, but as the weight of the aircraft increases, the distance of the flight area from people and property increases. Flights in **special category** require obtaining approval to perform an air operation, require completion of training in a drone training center, but allow for flights at short distances from people. **Certified category** refers to the unmanned transport of hazardous materials and people.

The regulations currently in force provide that the authority responsible for airspace management in Poland, i.e. The Polish Air Navigation Services Agency may designate the following geographical zones[22]:

[21] Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 *on unmanned aerial vehicle systems and third country operators of unmanned aerial vehicles,* NS. OJ. UE L 152, 11/06/2019; Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on *on regulations and procedures for the operation of unmanned aerial vehicles,* NS. OJ. UE L 152, 11/06/2019; Guidelines No. 24 of the President of the Civil Aviation Authority of 30 December 2020. *on the delimitation of geographical zones for unmanned aerial vehicle systems,* OJ. OJ. Civil Aviation Authority, 30 December 2020, item 78.

[22] See §3.1 Guidelines No. 24 of the President of the Civil Aviation Authority of 30 December 2020. *on the delimitation of geographical zones for unmanned aerial vehicle systems,* NS. OJ. Civil Aviation Authority, 30 December 2020, item 78.

1) **DRA-P** – prohibited area in which operations with UAV systems cannot be performed;

2) **DRA-R** – a restricted zone for UAV systems, in which operations with the use of UAV systems may be carried out with the consent and based on the conditions listed by the Agency or the authorized entity, at the request of which the geographical zone has been designated, including:

   a) **DRA-RH** – restricted zone for UAV systems with a high probability of obtaining approval for the operation;

   b) **DRA-RM** – the zone restricted for UAV systems with average probability of obtaining approval for the operation;

   c) **DRA-RH** – the zone restricted zone for UAV systems with a low probability of obtaining approval for the operation;

3) **DRA-T** – a zone restricted zone UAV systems, in which the Agency indicates the technical requirements to be met by the UAV system with which the operation is to be conducted; for the DRA-T zone, it is allowed to apply additional conditions for the performance of operations, with the obligation to obtain approval for the operation;

4) **DRA-U** – the geographic zone for UAV systems, in which the operations of UAV systems can take place only with the support of specific, verified services provided in this zone and under the conditions indicated by the Agency;

5) **DRA-I** – information zone for UAV systems, containing information necessary to ensure the safe performance of operations with the use of UAV systems, including navigational warnings.

In each of the above-mentioned zones, apply both different rules, and thus also limitations, for flying with unmanned aerial vehicles.

Drone geographic zones may be designated in Polish airspace on the application of[23]:

[23] See §3.1 Guidelines No. 24 of the President of the Civil Aviation Authority of 30 December 2020. *on the delimitation of geographical zones for unmanned aerial vehicle systems,* OJ. Civil Aviation Authority, 30 December 2020, item 78.

1) the Operational Commander of the Armed Forces, Commander in Chief of the Military Gendarmerie, Chief of the Air Traffic Services of the Polish Armed Forces, Head of the Internal Security Agency, Head of the Intelligence Agency, Police Commander in Chief, Commander in Chief of the Border Guard, Head of the National Treasury Administration or State Security Service Commander – due to the needs of activities or activities of special operational or exploratory importance, ensuring the security of the state or public order, carried out in order to implement statutory tasks by the Armed Forces of the Republic of Poland, the Internal Security Agency, the Intelligence Agency, the Police, the Border Guard, the National Revenue Administration or State Protection Service;

2) the Chief Police Commander, the Chief Commander of the State Fire Service or the Director of the Government Center for Security – due to the needs of the protection of critical infrastructure, prevention of the effects of natural disasters or their removal, saving human life or health;

3) the President of the Civil Aviation Authority – due to the implementation of statutory tasks;

4) the State Commission for Aircraft Accident Investigation – due to the implementation of statutory tasks.

It should be noted that due to the statutory responsibility for the security of CI facilities, the Head of the Internal Security Agency and the Director of the Government Security Center may apply for the designation of a drone geographical zone.

For the protection of CI facilities, the DRA-P zone is designated, in which flights are performed under the principles set out in different legal regulations. In *Guidelines No. 7 of the President of the Civil Aviation Authority* of June 9, 2021[24] the following entries can be found in Annex 1:

– „A pilot performing an UAS operation:
1) is particularly careful, avoids any action or omission that might:
d) pose a threat to the protected facilities, devices or areas ”(Chapter 1, Art. 1.3);

[24] Guidelines No. 7 of the President of the Civil Aviation Authority of 9 June 2021 *on modalities for UAS operations following the entry into force of the provisions of Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aerial vehicles*, NS. OJ. Civil Aviation Authority, 9 June 2021, item 35.

– ‚UAS operations in the' open ‚category shall be conducted under the following conditions:
5) in the DRA-P zone (...) – with the consent of the manager of a given zone and under the conditions specified for it"(Chapter 2, art. 2.1);
– „UAS operations in the" specific „category shall be performed under the conditions set out in Part B or C of the Annex to Regulation No 2019/947 / EU:
1) according to the standard scenarios (STS) published in Addendum 1 to the Annex to Regulation 2019/947 / EU, or
2) in accordance with the national standard scenarios (NSTS) published by the President of the Civil Aviation Authority in the Official Journal of the Civil Aviation Authority „(Chapter 3, Art. 3.1).

According with the STS or NSTS, flights in the DRA-P area are to be carried out „with the consent of the manager of the protected facility for that area and on the basis of the conditions specified for that area".

– ‚Operations in the visual range (VLOS), first person view (FPV) and out of the visual range (BVLOS) by an approved UAS shall be performed under the following conditions:
4) in the DRA-P zone (...) – with the consent of the manager of a given zone and under the conditions specified for it"(Chapter 3, art. 3.2).

On the basis of the above-mentioned regulations, flights in DRA-P zones are generally forbidden, but flights can be performed with the consent and based on the conditions specified by the zone administrator. This means, practically that the pilot of an unmanned aerial vehicle cannot fly in the DRA-P zone, but if this pilot performs the job for the needs of the zone manager, then such a flight is possible. The regulation is directed, for example, to the facility's physical security personnel, who may use unmanned platforms to supervise the facility.

5. Methods of protecting critical infrastructure against threats from unmanned aerial vehicles

The sequence of events that involve attack of object with an UAV can be presented in the diagram:

Diagram no. 1. A diagram of the sequence of events taking place in the course of an attack with the use of UAVs (author: Jędrzej Łukasiewicz).

The activation of the threat by the pilot consists in programming the platform with the use of software or activating the transmitting apparatus for communication between the aircraft and the pilot and directing the aircraft to the target. An attack can take place in various ways, and the most common attack methods include:

- use of the VIS camera,
- use of an IR camera,
- use of communication scanners,
- breakdown of the UAV with installation elements,
- transfer of an explosive charge,
- relocation of cargo containing harmful chemicals.

Examples of attack targets:

- observation / identification of devices that make up the physical protection system,
- observation of the activities of physical security personnel, obtaining information about procedures,
- identification of people employed in the protected facility,
- obtaining intelligence information concerning the technology used in the protected facility,
- eavesdropping on communications of physical security personnel or personnel employed in the facility,
- physical damage to the device used in the technological process in the facility,
- significant damage to devices, installations, paralysis of the facility's operation,
- causing environmental contamination in the facility or in the vicinity of the facility.

In the event that an IK facility equipped with an unmanned aerial vehicle detection system is detected anyway, steps can be taken to neutralize the attacking drone using the methods described earlier (see Chapter 3). The neutralization of the unmanned aerial vehicle may take place pursuant to Art. 126A of the Act of July 3, 2002 – *Aviation law*[25]. The unmanned aerial vehicle may be destroyed or the control may be taken over if:

1) flight mileage or UAS operation:

   a) threatens the life or health of a person,
   b) poses a threat to the protected facilities, devices or areas,
   c) disturbs the course of a mass event or threatens the safety of its participants
   d) poses a reasonable suspicion that it may be used as a means of a terrorist attack;

2) the unmanned aircraft performs a flight in the airspace in the part where flight restrictions have been introduced or located over the territory of the Republic of Poland, where the flight of the aircraft is prohibited from the ground level to a certain height.

[25] The Act of 3 July 2002 – *Aviation law,* Journal of Laws 2020, item 978, as amended)

Officers of the Police, Border Guard, Government Protection Bureau, Internal Security Agency, Foreign Intelligence Agency, Central Anti-Corruption Bureau, Military Counterintelligence Service, Military Intelligence Service, Customs and Revenue Service, and Prison, guards of the Marshal's Guard, soldiers of the Military Gendarmerie and the Armed Forces of the Republic of Poland, and employees of specialized armed security formations are entitled to destroy or immobilize an unmanned aircraft or take control of its flight.

Due to the conditions of use of anti-drone systems, as well as their effectiveness and the unpredictable consequences of a drone falling to the ground, measures to prevent attacks with the use of drones should be considered. Therefore, preventive actions can be presented by modifying the diagram presented above:

Diagram no. 2 A diagram of the sequence of events occurring in the course of an attack with the use of UAVs, taking into account preventive actions (author: Jędrzej Łukasiewicz).

The proposed preventive actions are:

1. Designation of geographic zones for UAVs

Designation of DRA-P geographical zones for unmanned aerial vehicles is a method that can increase the level of security of the protected facility. This method, however has quite a significant drawback. If a DRA-P zone is designated over an object, this would cause the information to be published in the aeronautical documentation. Thus, it would become open to everyone and would designate the location of the IK object. Thus, the decision to define the DRA-P zone over the CI facility should be made after a overall analysis of the rationality of such an operation. Analysis of that type must be based on the assumption that a terrorist does not attack the CI facility only because it is an CI facility, but rather due to the fact that the potential consequences for the state's continuity of operation would be significant. It seems right to begin the selection of the IK object over which the DRA-P zone should be pointed out, by defining the actual vulnerability of the protected facility to a potential drone attack. Not every IK object is vulnerable to such an attack, and the potential effects of such an attack may be negligible. If the object is susceptible to a drone attack, it is necessary to determine the value of the risk of threats and determine whether the risk is acceptable, tolerated or unacceptable. In the event of an unacceptable risk, preventive measures should be

taken to reduce the risk value to a tolerable or acceptable value. When selecting CI facilities that should be included in the DRA-P zone, one should focus on installations ensuring water supply as well as electricity generation and transmission installations. These installations play a significant role for the continuity of the state's operation, as well as for the health and life of citizens.

The risk value is calculated using a known formula[26]:

$$R = P_A \times P_S \times C$$

where: R – risk value, P_A – the probability of an attack on an object, P_S – the probability that if an attack with an unmanned aerial vehicle occurs, the attack will be successful for the attacker, C – consequences of the attack.

Installations for which the risk value of hazards is unacceptable should be surrounded by a DRA-P zone. Such a zone should be designed and demarcated in an appropriate manner. This means that the zone must be large and high enough. The currently published list of objects protected by zone P includes 31 items[27]. According to the flight conditions, if the horizontal boundaries of the DRA-P zone are located within 500 meters from the boundary of the protected facility, no flights are allowed in the area of such a designated zone – except for those carried out for the needs and with the consent of the zone manager. As a rule, an unmanned aerial vehicle can fly outside such a designated zone up to 120 meters from the nearest point on the ground. Plants, structures or other obstacles located on the ground do not constitute a physical barrier obscuring the image that can be recorded with the camera provided by the aircraft.

If the horizontal boundaries of the DRA-P zone are located more than 500 meters from the boundary of the protected facility, then at a distance of more than 500 meters from the boundary of the protected facility to the end of the zone, the unmanned aerial vehicle may fly up to 30 meters above the ground, provided that its mass does not exceed 900 g. Such a flight does not require the consent of the area administrator. Nevertheless, the low flight altitude and large distance from the protected object do not allow, due to terrain obstacles, to observe the object with the use of a camera. Any other flights operated for and with the approval of the zone manager are permitted.

[26] See *A Method to Assess the Vulnerability of US Chemical Facilities*, US Department of Justice, Office of Justice Programs, USA; Garcia ML, *Design and Evaluation of Physical Protection Systems*, Butterworth-Heinemann 2008.

[27] Announcement No.16 of the President of the Civil Aviation Authority of September 24, 2019. *on the list of managers of the facilities protected by zone P,* NS. OJ. of Civil Aviation Authority, 24 September 2019, item 66.

An unmanned aerial vehicle outside the zone, in an area where no zones have been designated, may fly up to a height of 120 meters from the nearest point on the ground. Flights at higher altitudes are possible with the approval of the aviation authorities.

Drawing. Diagram of the drone geographic zone DRA-P presenting flight rules (author: Jędrzej Łukasiewicz)

The above analysis presents that the further the horizontal borders of the DRA-P zone are located from the borders of the protected facility, the more difficult it is to observe the object with the use of a drone camera. Also, other methods of attacking the object, with a properly designated DRA-P zone, become more difficult.

2. Taking actions for the benefit of the local community

The locations of the P air zones designated for the protection of objects of particular importance for the continuity of the state's operations are published by the President of the Civil Aviation Authority. DRA-P drone geographic zones are designated within these zones. If such a zone is located in an inhabited area, it is worth increasing the possibilities of controlling the surroundings by using the help of local residents. Their favor can be won through the activities taken by the operator of the protected facility administrator, for the benefit of the local community.

Winning approval may involve such activities as:

- making Christmas greetings to seniors. Seniors, especially those who are no longer working, can focus their attention on controlling what is happening in their vicinity. Asking to inform about the presence of „strangers" or people trying to fly a drone can greatly speed up the reaction of security personnel to the unwanted behavior of a potential attacker,
- the manager of an object can fund scholarships for gifted teenagers. Linking young people by involving them in the problems of ensuring the safety of installations situated in the vicinity of their place of residence would be the most beneficial activity,

- organizing social actions, e.g. „cleaning up the world together”,
- education and systematic organization of meetings with pupils from nearby schools, organizing popular science lectures on the technology used in the installation in order to arise the interest of young people,
- inviting local residents to visit the protected object,
- charity actions, such as the purchase of equipment for nearby public buildings.

That activity should be promoted both in local and social media.

People living in the area of the protected facility should know the borderline of the DRA-P zone, beyond which no flights are allowed. Notifying the local inhabitants can be accomplished by means of leaflets, setting information boards or even via parish announcements. That sort of action would make sense if the residents simultaneously know the emergency telephone number to the facility security office.

3. Training of Police officers

An important action seems to be the training and regular supplementary training of officers of local Police units in the field of the Aviation Law and other legal regulations that may influence the manner of performing flights. Such additional legal acts include: regulations and guidelines of the President of the Civil Aviation Authority, acts: the Penal Code, the Code of Petty Offenses, the Atomic Law, on the protection of persons and property, on copyright and related rights, on nature protection, and on the protection of personal data. A Police officer aware of the abovementioned regulations would know how to hinder or prevent the flight of an unmanned aircraft in the area of the protected facility[28].

4. Full UVA pilot training for security personnel

An important element in the preparation of security personnel to ensure the security of the protected facility is complete training in the field of piloting unmanned aerial vehicles. Such training would be aimed at: making the personnel aware of the rules on which persons who are not employees of the installation may fly in the area of the facility, but also to prepare security personnel to fly both with the use of unmanned aerial vehicles (A) and multirotors (MR), in order to control foreground of the protected

[28] See. Art. 47 point 7 of the Act of May 24, 2013. *on measures of direct coercion and firearms*, Journal of Laws 2019, item 2418 i.e.

facility. The supervision could be performed with the use of cameras operating in the visible and infrared spectrum of electromagnetic radiation. The staff performing patrol flights could detect unusual activity in the area of the facility with the help of an UAV. The unmanned aircraft could be used for a long-term inspection of great areas (A), while the multirotor (MR) for point control of selected places where suspicious activity was observed.

5. Masking the elements of the protected object

In a lot of cases, preparation for an attack on a CI facility consists in an attempt to register employees' activity, obtain information about technology, and obtain information on technical equipment and physical protection procedures of the facility. Defense against an attempt to film activity on the premises of a protected facility may consist in building covers covering communication routes and important elements of the facility's installation equipment. Such covers can be painted in various patterns (graffiti) giving the impression of three-dimensionality of the recorded image.

6. Covering the elements of the object protected against the explosion of material transferred by the drone or against kinetic impact on the installation elements

In the case of potential CI facilities currently being designed in Poland, new sources of threats, such as unmanned platforms in the air, on land and under water, should be considered, and the facilities should be structured in such a way as to limit the consequences of a potential explosion of explosives. The effects of an explosion can be limited with the use of explosion-proof covers in the construction of the facility. It is necessary to consider, in the case of already existing objects, to cover sensitive elements of the installation with elements absorbing and dissipating the energy of a potential explosion or kinetic impact of an unmanned aircraft[29].

[29] Al-Rifaie, H .; Wellsski, R .; Gajewski, T .; Malendowski, M .; Sumelka, W .; Sielicki, PW A New Blast Absorbing Sandwich Panel with Unconnected Corrugated Layers — Numerical Study. Energies 2021, 14, 214, https://doi.org/10.3390/en14010214.

7. Inevitable and high flight penalties in DRA-P

The Aviation Law currently in force in Poland [NS. U. 2002 No 130 pos. 1112] there are penalties for flying in a manner inconsistent with the regulations. In this act we can find the following entry:

> Art. 212.1. Who:
> 1) when performing a flight with an aircraft:
> a) violates the air traffic regulations in force in the area in which the flight is being flown,
> c) violates, issued under Art. 119(2) 2 of the Act, prohibitions or restrictions on flights in Polish airspace introduced due to military necessity or public safety,
> – is subject to imprisonment of up to 5 years.

The strict application of this penalty to people who break the rules of flying in the DRA-P zone is a condition for increasing the security level of the protected facilities. An additional penalty should be the coverage of all costs related to the operation of services, security personnel, removal of the effects of a flight, etc. by the pilot of an unmanned aerial vehicle – analogous to the solutions used to punish the perpetrators of false reports on the planting of explosives.

6. Conclusions

» Establishing a working group at the Director of the Government Center for Security, consisting of nationally recognized civil and military specialists, which would be able to prepare expert opinions in the field of security of CI facilities (including also proposals to improve the current legal regulations), which could then be used by the Director of the GSC [Government Center for Security] to prepare recommendations for updating the National Critical Infrastructure Protection Program in this area.

» Preparation of the White Book of the results of the development of drone systems for the security of strategic facilities, critical infrastructure and those with a statute of special importance as part of an interministerial team made up of representatives of the RCB, Ministry of Interior and Administration, Ministry of National Defense, Chancellery of the Prime Minister, Ministry of Infrastructure, National Security Bureau, as well as external experts represented by national academic centers. The aim of tat team should be to define legal and organizational gaps blocking effective protection against this type of threats, as well as to develop minimum anti-drone security standards for the above-mentioned. objects – the already operating ones and the new designed ones.

» Establishment of a central national specialist laboratory responsible for testing anti-drone systems (land, air and water) and their certification for use in CI facilities. The laboratory should employ physicists, chemists, computer scientists, roboticists, electronics engineers, and former military soldiers with technical specializations. The laboratory could help to maintain the highest standards of devices used in the construction of the physical protection system of CI facilities.

» In view of the strategic investments currently underway in the country, such as the FSRU LNG terminal (*Floating Storage and Regasification Unit*), the Baltic Pipe gas pipeline, offshore wind farms in the Baltic Sea and the construction of a nuclear

power plant, as well as the construction of the Central Communication Port, a legal framework obliging the future investor of the IK facility to carry out a risk analysis (at the design stage), the source of which are unmanned drone platforms and the choice of location so that the anti-drone systems currently available on the market can be used. The facility's installations should also be designed to withstand a drone attack.

» Creation of a platform integrating Polish research projects related to anti-drone systems, with particular emphasis on the technology of UAV swarms, e.g. under the aegis of the Łukasiewicz Research Network.

Funded by the National Freedom Institute
– Center for the Development of Civil Society
from the Civic Organizations Development Program
for 2018–2030

National Freedom Institute
Centre for Civil Society Development

Civil Society
Organisations
Development Programme
for 2018–2030
CSODev

SECURITY
BEYOND DIVISION

www.PTBN.online