DOI: 10.4467/27204383TER.22.012.15428

ORCID: 0000-0002-7082-8511

JĘDRZEJ ŁUKASIEWICZ

Unmanned aerial vehicles as a source of threats to the state's electricity supply infrastructure and the proposed methods of protecting this infrastructure

Abstract

Unmanned aerial vehicles pose a threat to objects important to national security. Their versatility, resulting from the characteristics of individual types of aircraft, means that the scale of their use in attacks is virtually unlimited. The electricity supply system is extremely important for state security. Due to the vastness of transmission networks and a significant number of node points of these networks, the question should be asked to what extent this system is resistant to terrorist attacks, especially those carried out with the use of unmanned aerial vehicles. In this paper, the author analyses an attack consisting in causing a short circuit of the electrical system with the use of a copper wire suspended under an unmanned aerial vehicle. The implementation of the recommended protection methods described in the paper should lead to an increased level of safety of transmission networks.

Keywords:

unmanned aerial vehicles, power grid, protection of facilities critical to national security, anti-drone prevention

Unmanned aerial vehicles (UAVs) are a source of threats to facilities important to national security. Unmanned aerial vehicles (e.g. aircraft, multirotor or helicopter) are devices that perform their missions without the presence of a pilot on board. They can attack targets, including humans, using artificial intelligence algorithms[1]. Press releases reveal further examples of the use of UAVs in warfare, but also in terrorist attacks[2], including on the electricity supply system. The aim of the analysis presented in this paper is to determine the vulnerability of the power grid to attacks carried out by unmanned aerial vehicles and to identify methods of preventing attacks carried out by such devices on power facilities in Poland. Conducting such an analysis seems justified as media reports entitle to formulate the hypothesis that the success of one such attack may cause a trend towards drone attacks on power grid facilities in Europe, including Poland.

Structure of the power grid in Poland

Electricity in Poland is produced by thermal, hydro, wind, photovoltaic, biogas and biomass power plants; some electricity is imported from abroad[3]. Electricity from the producer to the end user is transmitted through the power grid, consisting of lines and substations. Every transmission of energy generates losses. To keep these losses as low as possible, transmission networks with voltages between 220 kV and 400 kV, known as the highest voltages, are used for long-distance transmission of electricity. For transmission of electricity over distances of up to several tens of kilometres, lines with a voltage of 110 kV are used. This is a high voltage. In local distribution lines, the voltage is between 10 kV and 30 kV and this is called medium voltage. The medium voltage is transformed to a low voltage of 220/230 V or 380/400 V. The low voltage

[1] https://www.newscientist.com/article/2278852-drones-may-have-attacked-humans-fully-autonomously-for-the-first-time/ [accessed: 30 XI 2021].

[2] https://edition.cnn.com/2019/03/14/americas/venezuela-drone-maduro-intl/index.html [accessed: 30 XI 2021]; https://www.bbc.com/news/world-middle-east-59195399 [accessed: 30 XI 2021]; https://www.reuters.com/world/middle-east/iran-backed-militia-behind-attack-iraqi-pm-sources-2021-11-08/ [accessed: 30 XI 2021].

[3] *Energetyka, dystrybucja, przesył* (Eng. Energy, distribution, transmission), PTPiREE, http://ptpiree.pl/raporty/2021/raport_ptpiree_2021.pdf [accessed: 30 XI 2021].

is used by the end customer[4]. The plan of the power grid in Poland, including planned investments, is presented in Figure 1.

Fig. 1. Diagram of the power grid in Poland.

Source: https://www.pse.pl/obszary-dzialalnosci/krajowy-system-elektroenergetyczny/plan-sieci-elektroenergetycznej-najwyzszych-napiec/planowana [accessed: 30 XI 2021].

The power system in Poland consists of system substations for extra-high voltage, distribution substations for high voltage and transformer substations. According to information provided by Polskie Sieci Energetyczne SA, 281 extra-high voltage lines with a total length of 15 316 km and 109 extra-high voltage substations are currently operated in Poland. The high, medium and low voltage lines are managed by: Enea Operator, Energa-Operator, Polska Grupa Energetyczna Dystrybucja, Innogy Stoen Operator and Tauron Dystrybucja. The total

[4] https://www.pse.pl/obszary-dzialalnosci/krajowy-system-elektroenergetyczny/informacje-o-systemie [accessed: 30 XI 2021].

length of connections managed by the aforementioned operators is 169,076 km. The operation of the aforementioned lines required the construction of 111 extra-high voltage, 1,537 high voltage and 262,989 medium voltage substations[5]. The highest voltage lines and the high voltage lines are made of cables that are not insulated. Medium voltage lines are usually not insulated. Insulation is used on medium voltage lines when they run through a forest. Low voltage lines are insulated[6]. Overhead lines are equipped with remote-controlled disconnectors and short-circuit alarms, which allow a fault to be located quickly.

Damage to an electrical installation by means of an unmanned aerial vehicle

Threats to electricity networks have long been recognised[7], with reports of attacks on network components appearing in the media[8].

On 4 November 2021, the information contained in the Joint Intelligence Bulletin (JIB) report was published. In it, the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI) and the National Counterterrorism Center (NCTC) referred to an incident that occurred in the United States of America, in Pennsylvania, which involved an attempted attack on elements of the electrical grid using a drone with an electrical wire suspended from its enclosure. The attack most likely involved an unmanned aerial vehicle manufactured by DJI Mavic 2[9]. This is a model commonly available in shops.

In connection with the disclosure of information about the possibility of attacking the power grid with an unmanned aerial

[5] *Energetyka, dystrybucja, przesył...*, pp. 33–49, 2021 [accessed: 30 XI 2021].

[6] Ibid., pp. 51–67, 2021 [accessed: 30 XI 2021].

[7] P.W. Parfomak, *Physical Security of the U.S. Power Grid. High-Voltage Transformer Substations,* Congressional Research Service, 17 VI 2014; R. Baldick, B. Chowdhury, I. Dobson, *Initial review of methods for cascading failure analysis in electric power transmission systems IEEE PES CAMS task force on understanding, prediction, mitigation and restoration of cascading failures,* in: *IEEE Power and Energy Society General Meeting – Conversion and Delivery of Electrical Energy in the 21st Century*, 2008.

[8] https://www.wsj.com/articles/SB10001424052702304851104579359141941621778 [accessed: 30 XI 2021].

[9] https://www.thedrive.com/the-war-zone/43015/likely-drone-attack-on-u-s-power-grid-revealed-in-new-intelligence-report [accessed: 30 XI 2021].

vehicle, a question should be asked to what extent the power grid in Poland is susceptible to such an attack.

For the analysis of the possibility of damaging the grid with an unmanned aircraft, devices whose flight parameters are similar to models commonly available on the market were selected. It should be assumed that some models are designed to perform only specific types of missions, e.g. in the case of models carrying a camera, such a mission is to film an object, while other types of aircraft are universal platforms, adapted by the manufacturer to lift any payload, whose only limitation is its size and weight. Such a payload could be, for example, an air quality device, a lidar system, but also an explosive. Aircraft designed to perform a specific mission are compact, enclosed structures, and it is somewhat difficult to suspend additional payloads underneath them. Vessels that are universal platforms are open structures with decks specially prepared for the suspension of cargo. Analysing the parameters of platforms generally available on the market, it may be assumed to some extent that in most cases an aircraft can lift an additional load of approx. 30% of the weight of the platform without equipment. Platforms that can lift the following cargo weights have been selected for analysis: 0.25 kg, 0.50 kg, 2.5 kg and 4.0 kg. As the weight of the payload increases, the size of the aircraft also increases, so there is a difficulty in transporting and concealing it.

Damage to the electrical system and thus stopping its operation can be done in various ways: it can be mechanical damage by detonation of an explosive charge, damage by causing a short-circuit of live wires to earth, known as grounding, and damage by causing a short-circuit of live wires, with the short-circuit occurring between different phase wires. The November 2021 press release describes an attempted attack involving an induced short circuit in the electrical system, so two scenarios were chosen for analysis:

1. An unmanned aerial vehicle with a long, uninsulated electrical wire suspended from it flies up to the uninsulated phase wire and short circuits it to the ground;
2. An unmanned aerial vehicle with a long uninsulated electric wire suspended flies up to a pole with uninsulated electric wires and short circuits the wires.

Determination of the length of an uninsulated copper conductor which will be used to create a short circuit in an electrical installation

A short circuit will occur between one of the phase conductors and ground or between phase conductors. The length of an electrical conductor that will serve to create a short circuit in an electrical installation can be determined from the formula:

$$l = \frac{m}{\sigma \times S}[\mathrm{m}]$$

where:
l - length of the conductor expressed in m,
m - mass of the wire expressed in kg which the unmanned aerial vehicle will lift up,
σ - density of the material expressed in kg/m3; the density of copper is 8920 kg/m^3,
S - cross-sectional area of the material expressed in m^2.

The cross-sectional areas of electrical conductors are standardised quantities. Calculated lengths of conductors constituting an additional charge with masses: 0.25 kg, 0.5 kg, 2.5 kg, 4.0 kg, are listed in Table 1.

Table 1. Summary of the lengths of the electric cables suspended under the unmanned aerial vehicle, with given cross-sections and assumed masses.

Conductor cross-sectional area S [mm²]	**Length of cable as additional aircraft payload [m] depending on the mass of the cable suspended from the unmanned aircraft**			
	0,25 [kg]	**0,50 [kg]**	**2,50 [kg]**	**4,00 [kg]**
0,50	55,7	111,5	446,3	892,6
0,75	37,1	74,3	297,5	594,8
1,00	28,5	56,9	227,7	455,4
1,50	18,2	36,4	145,7	291,5
2,50	11,0	22,0	88,2	176,3
4,00	7,1	14,2	56,9	113,8
6,00	4,5	9,1	36,4	72,9
10,0	2,7	5,5	22,0	44,02
16,0	1,7	3,5	14,1	28,2
25,0	1,1	2,2	8,9	17,9
35,0	0,8	1,6	6,4	12,9
50,0	0,5	1,1	4,5	8,9

As can be read from Table 1, for cross-sectional areas up to 4 mm^2 the length of the cable that can be suspended from the UAV is sufficient to cause a short circuit of the phase conductors on the pole. For smaller conductor cross-sections, its length will be sufficient to make a short circuit - a grounding - between the phase conductor and the earth. When a cable suspended from an unmanned aerial vehicle is suspended from the phase conductor of an electrical installation, a short circuit will occur and a short-circuit current will flow through the short-circuiting wire. Such a wire may melt, and the approximate time of melting will depend on its cross-sectional area and the short-circuit current[10]. The approximate values of the currents that will cause the conductor to melt in the declared time are listed in Table 2. This approximation results from the different cross-sectional area S of the conductors used in the United States.

Table 2. List of approximate currents which will cause the conductor to melt after the declared time for the given cross-sections.

Cross-sectional area of the conductor S [mm^2]	**Approximate value of the electric current flowing in the declared time until conductor melting [A] depending on the time of the electric current flow**		
	10 s	**1 s**	**32 ms**
0,50	58,5	158	882
0,75	83,0	250	1400
1,00	99,0	316	1800
1,50	140,0	502	2800
2,50	198,0	798	4500
4,00	280,0	1 300	7100
6,00	396,0	2 000	11 000
10,0	561,0	3 200	18 000
16,0	795,0	5 100	28 000
25,0	1 100	8 100	45 000
35.0	1 300	10 200	57 000
50.0	1 900	16 000	91 000

[10] W.H. Preece, *On the Heating Effects of Electric Currents. No. II*, „Proceedings of the Royal Society of London" 1887–1888, vol. 43; W.H. Preece, *On the Heating Effects of Electric Currents. No. II*, „Proceedings of the Royal Society of London" 1887–1888, vol. 44; E.R. Stauffacher, *Short-time Current Carrying Capacity of Copper Wire*, „General Electric Review" 1928, vol. 31, no. 6.

The fault tripping times are described in the technical documentation[11] and are 120 ms for 400 kV and 220 kV networks and 150 ms for 110 kV networks, respectively. The currents flowing through the lines vary greatly and depend among other things on the type of line. The maximum values of the measured currents can reach up to 1152 A[12]. This means that practically each of the conductors indicated in the table should melt before the line protections are switched off. In the case of an attack on high-voltage distribution substations and transformer stations, which are complex installations not protected from above, the consequences of an attack may be more serious. However, due to the complexity of the construction of the above installations shown in Figure 2, it is difficult to estimate the extent to which elements of the installation will be damaged.

Fig. 2. 400/110 kV high-voltage switching station.

Source: https://elbud.katowice.pl/pl,30,3,projekty-rozbudowa-stacji-400_110-kv-dobrzen.html [accessed: 30 XI 2021].

[11] PSE Operator SA, *Standardowe Specyfikacje Funkcjonalne. Elektroenergetyczna automatyka zabezpieczeniowa, pomiary i układy obwodów wtórnych* (Eng. Standard Functional Specifications. Electricity protection control, metering and secondary circuits), Warszawa 2010 (update 2012).

[12] M. Jaworski, M. Szuba, *Analiza obciążeń napowietrznych linii najwyższych napięć w aspekcie wytwarzania pola magnetycznego* (Eng. Load analysis of overhead high-voltage lines in terms of magnetic field generation), „Przegląd Elektrotechniczny" 2015, no. 5.

The consequences of damage to transmission lines or servicing stations may be similar to those observed during the failure at the Rogowiec substation (through which the power plant in Bełchatów is connected to the national grid system). As indicated in the report[13], the cause of the failure was human error, which led to a short circuit in the electrical system. As a result of the failure, most of the units of the Bełchatów Power Plant were switched off.

It is worth mentioning that there is no ban on flying over transmission lines. The law[14] only stipulates that operations carried out with the use of unmanned aerial vehicles of open and special category over power lines and other devices located in open terrain, the destruction or damage of which may pose a threat to human life or health and the environment or cause serious material losses, shall be carried out with special caution.

Methods of detection of unmanned aerial vehicles

The most commonly used UAV detection methods include:

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

None of these methods used alone can be relied upon to detect a flying object. Therefore, UAV detection systems are made up of different detection devices, operating on different principles. Currently, many companies are developing anti-drone systems, so it is to be expected that their sales will also increase due to the growing number of UAVs.

[13] https://businessinsider.com.pl/wiadomosci/awaria-elektrowni-belchatow-pse-podaje-przyczyny/qpp086b [accessed: 30 XI 2021]; https://www.teraz-srodowisko.pl/aktualnosci/elektrownia-belchatow-awaria-stacja-rozdzielcza-PSE-10340.html [accessed: 30 XI 2021]; https://www.cire.pl/artykuly/serwis-informacyjny-cire-24/184908-poniedzialkowa-awaria-odlaczyla-od-sieci-niemal-cala-elektrownie-belchatow [accessed: 30 XI 2021]

[14] *Guideline No. 7 of the President of the Civil Aviation Authority of 9 June 2021 on the modalities of operations using unmanned aircraft systems in view of the entry into force of the provisions of Commission Implementing Regulation (EU) No 2019/947 of 24 May 2019 on rules and procedures for the operation of unmanned aircraft.*

As the functionality of UAVs increases, the functionality of anti-drone systems is also changing.

Detecting a vessel using radar is a method familiar from manned aviation. However, the radars used to detect drones are different from those used to detect manned aircraft. The latter detect objects with a larger beam reflecting area and a higher progressive speed than unmanned aircraft[15]. The advantage of this method is that it can detect an attack when it is carried out at high altitudes. Radar will effectively detect an aircraft if there are no obstacles between the radar antenna and the flying aircraft. It will also detect the passing of an unmanned aircraft if it is far from the radar antenna. Unfortunately, the disadvantage of this method of detection is that an unmanned aircraft using a lidar distance measurement system, including distance from the ground, may be travelling just above the surface. In such a situation, the radar system will not detect the flying UAV. The same lidar system will allow the drone to detect and avoid terrain obstacles. The market is currently quite saturated with anti-drone radar systems[16]. However, it seems that attempts to detect a drone flying in a densely built-up area will be mostly ineffective.

An unmanned aircraft can also be detected by monitoring the communication-control between the flying unmanned platform and the ground station. Among the most common methods of controlling an unmanned aircraft is control using a transmitting apparatus, the so-called transmitter, which is located on the ground, in the hand of the pilot. Such apparatus is equipped with two sticks allowing to control the platform in each direction and a set of switches and knobs allowing to operate additional on-board devices. For example, the knobs can be used to control a gimbal with an on-board camera, and a set of switches can be used to control other devices, such as a raised landing gear or a key that releases a suspended load, allowing the load to be dropped at a desired location. Communication between the transmitter and the UAV's computer can take place at two frequencies: platform control at 2.4 GHz and camera image transmission at 5.8 Ghz. In typical solutions, this control method allows control of the UAV over a distance of up to about 3 or 4 kilometres.

[15] https://www.defence24.pl/dlaczego-konflikt-w-gorskim-karabachu-powinien-zmienic-wojsko-polskie [accessed: 30 XI 2021].

[16] https://www.hertzsystems.com/en/antidrone-systems/ [accessed: 30 XI 2021].

The second method of controlling the platform is to send commands from the ground to the computer controlling the UAV via a ground computer and a tablet using what is known as a telemetry channel. Telemetry is a two-way communication channel responsible for transmitting aircraft parameters from the platform to the ground, including such parameters as position, altitude, horizontal progress velocity, rate of climb or descent, battery charge status, as well as forward or backward tilt and left or right roll. Telemetry also allows a command from the pilot to be sent to the aircraft. Such a command can be defined on the ground by drawing in the telemetry software a given geographical position of the platform, its height at a given position, the progressive speed the platform should achieve on its way to the next position, and the so-called POIs (*Point of Interest*), i.e. points towards which the unmanned aircraft should point the camera lens during flight. Communication between the aircraft and the pilot takes place through this channel on different frequencies, e.g. 433 MHz or 868 MHz. The communication distance using telemetry is longer than the communication distance using 2.4 GHz or 5.8 GHz frequencies and can be even above 20 kilometres. An unmanned flying platform can also be controlled by using GSM networks. A schematic of such a control system is shown in Figure 3.

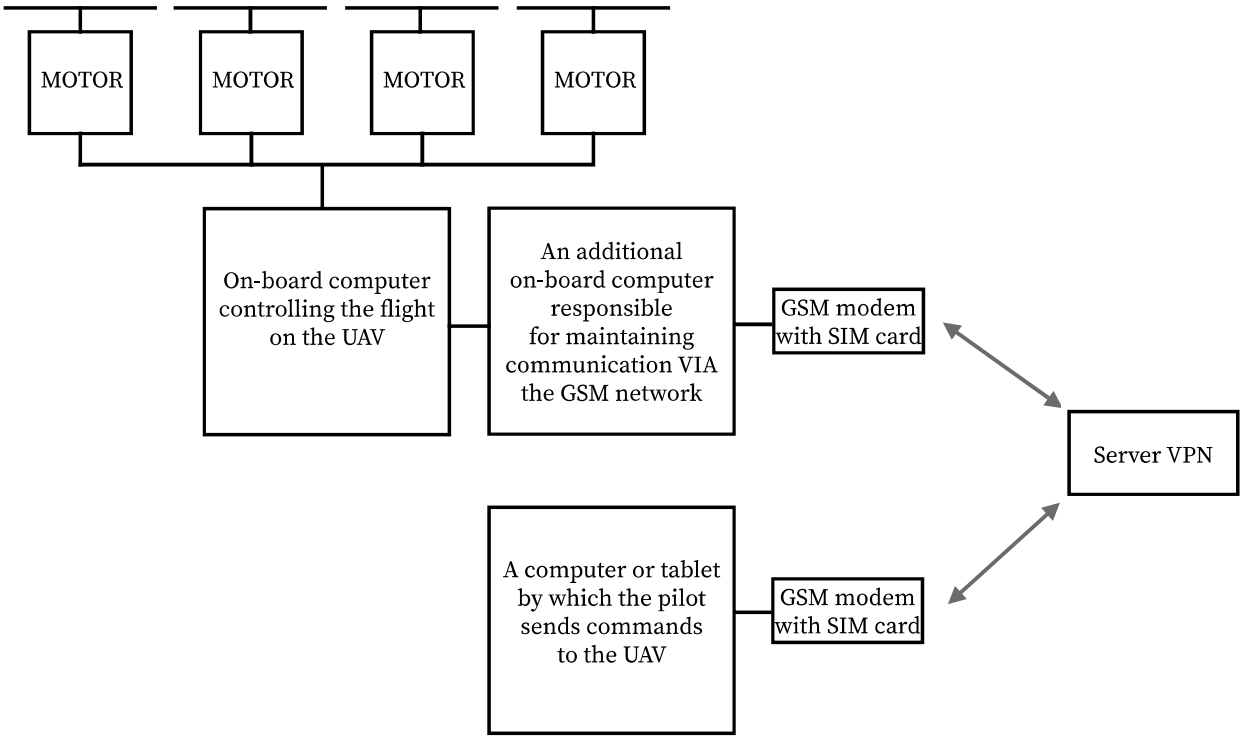

Fig. 3. Scheme of communication between the unmanned aerial vehicle and the pilot via the GSM network.

Source: Author's own elaboration.

GSM communication makes it possible to control an unmanned aircraft without distance limitations. The pilot of the aircraft can control it from any place on earth. The only condition to realise such a connection is the access to the GSM network of both the pilot and the aircraft. The communication is realised through a VPN server, so it is an encrypted communication.

Current detection systems for flying UAVs control the frequency spectrum of electromagnetic radiation in the region of the detector location. Since standard UAVs use electromagnetic radiation of known frequencies to communicate with the pilot, the detector can detect the appearance of a source of emission of such radiation. It is possible to use artificial intelligence and machine learning technologies to indicate to the detector which sources are drones and which are not[17]. It is worth noting that these systems can detect UAVs that maintain communication with a ground station during flight. They usually detect typical aircraft, commonly available on the shelves. However, they become ineffective when the aircraft has been programmed before take-off and flies without communicating with the base station, or maintains communication with the base station at unusual frequencies. Additionally, the electronic elements of which the drone is composed can be separated from the environment by a so-called Faraday cage, which prevents the penetration of electromagnetic radiation into the aircraft and from its interior to the outside. It cannot then be detected because the Faraday cage isolates it from the electromagnetic radiation detectors. Monitors controlling the operation of selected aircraft models can be used to detect typical aircraft. Such monitors include the AeroScope device, which can detect communication and aircraft status in real time. However, such a device only detects drones made by DJI[18]).

Another method of unmanned aircraft detection is based on the detection of noise originating from their rotating components. In UAVs, the sources of noise are propellers and, to a lesser extent, engines. Every flying UAV emits sound, with the frequency and intensity of the sound wave depending on the shape of the propeller

[17] https://www.droneshield.com/ [accessed: 30 XI 2021]; https://www.dedrone.com/ [accessed: 30 XI 2021]; https://www.echodyne.com/security/counter-drone-radar/ [accessed: 30 XI 2021].

[18] https://www.dji.com/pl/aeroscope [accessed: 30 XI 2021].

and the angular speed at which the propeller rotates. There are methods to reduce the noise emitted by unmanned aircraft[19]. These include the use of propulsion units with lower rotational speeds, the use of propellers with different numbers of blades, the use of propellers with different aerodynamic profiles. An unmanned aircraft may therefore go undetected if it emits low noise levels and flies where other noise sources are present, such as public transport vehicles, manned aircraft during take-off and landing, other man-made noises. It should also not be forgotten that an aircraft like an aeroplane can approach a protected object by gliding flight, so it will not be a source of propeller noise.

The last significant method of identifying unmanned aircraft is space analysis using cameras operating in both visible and infrared spectrums. Image analysis is carried out using a computer system which, based on the image recorded by the camera, recognises whether the flying object is a drone or, for example, a bird. Visual detection systems are based on machine learning and artificial intelligence technology. Teaching a computer to recognise an object is a tedious, time-consuming process that requires high computing power and a large database of source images depicting the object to be detected. Such systems detect typical aircraft. Once an aircraft has an unusual shape, it will be impossible to detect. Unmanned aerial vehicles can be built so that the shapes are very unusual. For example, Greenpeace members famously built a Superman-shaped drone and crashed it into a concrete reactor shield at the Bugey nuclear power plant in France[20]. The moment of the attack is shown in Figure 4. The drone itself hitting the wall of the reactor shield did not endanger the safety of the reactor.

[19] F.B. Metzger, *An Assesment of Propeller Aircraft Noise Reduction Technology*, NASA Contractor Report 198237, 1995; W. Yuliang et al., *Noise Reduction of UAV Using Biomimetic Propellers with Varied Morphologies Leading-edge Serration*, „Journal of Bionic Engineering" 2020, vol. 17, pp. 767–779.

[20] https://www.reuters.com/article/uk-france-nuclear-greenpeace-idUKKBN1JT17G [accessed: 30 XI 2021].

Fig. 4. The moment of attack on a nuclear reactor using a Superman-shaped drone.

Source: https://www.reuters.com/article/uk-france-nuclear-greenpeace-idUKKBN1J-T17G [accessed: 30 XI 2021].

Such walls are built to withstand the impact of a manned aircraft which, flying at high speed and possessing a large mass, would hit the target with high kinetic energy. However, this case has shown how irresistible protected facilities are to drone action, especially those built at a time when drones were not yet so widely available. Cameras operating in the visible band of electromagnetic radiation are unable to detect flying aircraft in low visibility conditions. Analysing space with cameras operating in the infrared range of electromagnetic waves makes it possible to detect heat sources other than those naturally found in space. An infrared camera can detect and distinguish an unmanned aircraft because it uses components that emit heat during operation. Such components can include both electric and internal combustion engines, as well as lithium-polymer batteries, which spontaneously heat up during operation. An infrared camera can detect a flying aircraft at night. However, also this way of detecting drones is not always effective. Knowledge of manned aviation indicates that it is possible to build the aircraft in such a way that the heat energy is dissipated to a large extent, so that the aircraft cannot be detected.

Selected methods to neutralise unmanned aircraft

The process of detecting an unmanned aircraft itself is only the first stage of defence against its attack. The following methods are used to neutralise hostile UAVs:

- hitting and entangling the moving parts of the UAV with a net,
- interference with the positioning of the satellite system used by the aircraft,
- interference with aircraft-ground station communications,
- use of high-power laser light,
- damage to electronic systems by high-power electromagnetic pulse.

Hitting and entangling an unmanned aircraft is a difficult process. The attacking aircraft may be a multirotor craft, an aircraft or a helicopter. It can also combine features of all the above-mentioned types and then a hybrid of them is formed. Such hybrids include aircraft with vertical take-off capability, the so-called V-tol (from Vertical Take Off and Landing). Each of these devices has different physical characteristics, against which the method of neutralisation with a net will be ineffective. Such characteristics certainly include the progressive speed of the ship in flight. An aircraft moves at a high speed, while a multirotor moves at a relatively low speed. The throwing device may be in the hand of a member of the site security staff or it may be suspended from another aircraft piloted by a member of the site security staff. Mesh systems used to neutralise aircraft are effective when the attacking aircraft is moving at low speed or remains in a so-called hover. The main problem when using this method is the short distance of the net throwing device from the target. After a successful hit, an unmanned aircraft entangled in the net falls to the ground with the help of a parachute system. Thanks to its low speed of descent, it will not crash to the ground, damage infrastructure elements or cause loss of health or life if it falls on a person. An undamaged aircraft with a computer on board can provide evidence for a court if the perpetrator of an attack is discovered.

Another method of neutralising a flying aircraft is to jam or impersonate the satellite positioning system signal. The interference or impersonation of a satellite signal is reported in the press[21].

[21] https://www.techtarget.com/searchsecurity/definition/GPS-jamming [accessed: 30 XI 2021]; https://www.militaryaerospace.com/rf-analog/article/14207023/gps-

The interference is when a signal is emitted from the interfering device at the frequencies on which the positioning system operates. The jamming signal is more powerful than the satellite signal. In such a situation, the satellite receiver used for navigation on board the unmanned aircraft considers the signal of the jamming device as correct and is not able to determine its position properly using that signal. Impersonation is when the impersonating device emits a signal containing a false position. In this way, the aircraft, instead of reaching its target, will fly to the place indicated by the neutralising device and the attack will be ineffective. The answer to this defence can be navigation, which allows to determine the position of the aircraft without access to the positioning system signal. Such navigation also allows an unmanned aircraft to fly through buildings or mines[22]. Non-satellite based navigation systems identify the position of the aircraft by means of lidar readings, ultrasonic distance measuring devices, visible or infrared camera systems[23]. Systems for navigation in the absence of access to satellite signals will develop rapidly due to the possibility of damage to satellites in the event of war[24]. A method of navigation without the use of satellite positioning system is also the deployment of ground stations emitting a position signal and navigation based on triangulation[25].

The devices interfering with the communication signal between the aircraft and the ground station emit high-power electromagnetic radiation at different frequencies, which include the frequencies used by the unmanned aircraft. Interference with communication takes place through the emission of an electromagnetic wave with a completely flat spectrum and noise intensity uniform throughout the jammed

signals-jamming [accessed: 30 XI 2021]; https://www.c4isrnet.com/newsletters/military-space-report/2020/04/15/natos-new-tool-shows-the-impact-of-gps-jammers/ [accessed: 30 XI 2021].

22 https://polskiprzemysl.com.pl/przemysl-energetyczny/gornictwo-urzadzenia-maszyny/drony-w-kopalniach/ [accessed: 30 XI 2021].

23 F. He et al., *Automated Aerial Triangulation for UAV-Based Mapping*, „Remote Sensing", December 2018, no. 10 (12), 1952.

24 https://spidersweb.pl/2021/11/rosja-satelita-smieci-kosmiczne.html [accessed: 30 XI 2021].

25 R. Kapoor et al., *UAV Navigation Using Signals of Opportunity in Urban Environments. An Overview of Existing Methods*, 1st International Conference on Energy and Power, ICEP 2016, 14–16 December 2016, Melbourne, Australia.

band. This is known as white noise[26]. This uniformity means that for each frequency of electromagnetic noise the power of emitted wave is the same. Such noise drowns out communication between aircraft and pilot, making control impossible. Interference systems can be circumvented quite simply, i.e. by using unusual frequencies not used in commonly available aircraft for vessel-pilot communication or by hiding the aircraft's electronic equipment in a so-called Faraday cage. Another method to prevent the aircraft from being neutralised is to program the mission before the flight and perform the flight in an autonomous manner, i.e. without the pilot's involvement, based on commands given before take-off.

The use of a high-power laser beam is an effective method under the right conditions. The laser light illuminates the flying aircraft and causes it to light up. This method is currently being developed in many countries[27]. The advantage of this method of destroying a drone is that it can be brought down from a relatively long distance. The disadvantages of the system are: the requirement to power the laser from a high-power source, sensitivity to weather conditions, including fog or rain. The system can destroy UAVs one at a time. When an attack is carried out with multiple drones or even with a swarm, this system has limited effectiveness.

Damaging electronic systems with a high-powered electromagnetic pulse is a technique known from military applications. An unmanned aerial vehicle is a technical object that uses systems of advanced electronics. Electronic devices used in drones include a control computer, an auxiliary computer that can be used to perform calculations such as image analysis, electronic controllers of the rotation of aircraft engines, receivers used to receive commands from the pilot, telemetry devices used to exchange information between the craft and a ground station, e.g. the status of the aircraft, satellite navigation devices, etc. Aircraft may be protected against electromagnetic pulse by using multilayer trays to shield electronic equipment from the impulse.

---

[26] B. Carter, R. Mancini, *Op Amps for Everyone,* Burlington 2009, pp. 174–175.

[27] https://www.rafael.co.il/worlds/air-missile-defense/c-uas-counter-unmanned-aircraft-systems/ [accessed: 30 XI 2021]; https://www.thedefensepost.com/2021/07/09/france-anti-drone-laser/ [accessed: 30 XI 2021]; https://www.aerospacetestinginternational.com/news/defense/us-air-force-progresses-testing-of-anti-drone-laser-weapons.html [accessed: 30 XI 2021].

All the methods mentioned above are of limited effectiveness, so it is necessary to look for other ways of protecting the object. Prevention, preventing the start of an attack, is important for the security or defence of the state. Such methods include:

- securing the protected object with a DRA-P zone,
- using devices which cut off the possibility of flying in the protected area,
- training of police officers in aviation law, procedures in force in unmanned aviation and regulations allowing for punishment of pilots flying illegally,
- training of facility security staff in piloting multirotor vessels and aircrafts,
- masking the elements of infrastructure of the protected facility,
- covering elements of the infrastructure from impact or from the effects of explosive cargo carried by aircraft,
- actions for the benefit of the local community.

Securing a protected facility with a DRA-P zone

According to the current guidelines of the President of the Civil Aviation Office (ULC)[28], the Polish Air Navigation Services Agency (PAŻP) may designate the following drone geographical zones:

a) DRA-T - a zone in which the flight of an unmanned aircraft is possible after the aircraft meets the technical requirements indicated by the PAŻP. In this zone, it is allowed to meet additional conditions for flight, including for example the requirement to obtain a permit to fly;
b) DRA-U - a zone where flight of an unmanned aircraft may only take place with the support of services required for this zone and under conditions of flight performance indicated by PAŻP;
c) DRA-I - information area, where the approval for flight is not required but where information is required to ensure flight safety;

[28] See: *Wytyczne nr 7 Prezesa Urzędu Lotnictwa Cywilnego z dnia 9 czerwca 2021 r...*

d) DRA-P - prohibited area, in which operations with unmanned aircraft systems may not be conducted;
e) DRA-R - restricted area for unmanned aircraft systems, in which operations with unmanned aircraft systems may be performed with the permission and under conditions specified by PAŻP or an authorised entity, at the request of which the geographical area was designated.

The DRA-R zone may consist of additional sub-zones designated by:

1. DRA-RH - in which the probability of obtaining permission to fly with an unmanned aircraft is high (*high*);
2. DRA-RM - in which the probability of obtaining permission to fly with the unmanned aircraft is medium (*middle*),
3. DRA-RL - in which the probability of being cleared to fly with the unmanned aircraft is low (*low*).

Due to the needs of actions or activities of particular operational or reconnaissance importance for ensuring national security or public order, conducted in order to carry out statutory activities, the geographical zones may be designated on the motion of the Operational Commander of the Armed Forces, Commander-in-Chief of the Military Police, Chief of the Air Traffic Services of the Polish Armed Forces, Head of the Internal Security Agency, Head of the Foreign Intelligence Agency, Police Commander-in-Chief, Commander-in-Chief of the Border Guard, Head of the National Revenue Administration or Commander of the State Protection Service. Due to the need to protect critical infrastructure facilities, prevent the effects of natural disasters or their removal, save human health or life, the geographical zones may be designated at the request of the Police Commander-in-Chief, the Commander-in-Chief of the State Fire Service or the Director of the Government Centre for Security.

Uniform rules on the operation of unmanned aircraft currently apply throughout the European Union[29]. According to these rules, flights by unmanned platforms are performed in three different categories. Each category corresponds to a certain level of risk

[29] *Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on rules and procedures for the operation of unmanned aerial vehicles; Commission Implementing Regulation (EU) 2020/746 of 4 June 2020 amending Implementing Regulation (EU) 2019/947 as regards the postponement of the dates of application of certain measures in relation to pandemic COVID-19 (OJ EU L 176 of 5 VI 2020, p. 13).*

associated with the mission. There are three levels of risk: low, for the OPEN category; medium, for the SPECIFIC category; and high, for the CERTIFIED category. The certified category includes flights carrying persons or dangerous goods. The SPECIFIC category are flights which require, in principle, consent to conduct the operation. Such consent, as implied, is given to pilots holding the appropriate rating to fly under the so-called standard scenarios. Standard scenarios are a set of rules of flight whose observance guarantees that the mission is performed with an acceptable risk. Currently in Poland, there are eight standard scenarios concerning flights within visual range (VLOS) and beyond visual range (BVLOS) for aircraft such as aeroplanes, multirotors and helicopters with take-off mass up to 4 kg and for aircraft such as aeroplanes, multirotors and helicopters with take-off mass not exceeding 25 kg. The open category is low-risk flights and therefore no flight approval is required. Pursuant to *Guideline No 7*, flights in the open category and in the special category in the DRA-P drone geographical zone shall take place with the consent of the zone manager and under the conditions specified for that zone. *Guideline No 7* does not include rules for flights in the certified category. The analysis of aviation documentation contained in the messages of the DroneRadar application (DroneRadar is an application for the Android and iOS systems, free and widely available in the shops of mobile network operators) indicates that in the DRA-P zones designated over protected objects, flights with unmanned aerial vehicles are allowed, but only up to a height of 30 m above the ground with an aircraft weighing not more than 0.9 kg and at a distance of not less than 500 m from the border of the protected object. These provisions indicate that DRA-P zones can be used to protect facilities, provided they are properly designed.

Let us consider two cases of DRA-P zones designated as in Figure 5.

1. The boundaries of the DRA-P zone are located at a distance "L" of less than 500 m from the boundaries of the protected object. Outside the zones, according to the general rules of flight, an unmanned aircraft can fly up to an altitude "H" of no more than 120 m above the ground. Using the Pythagorean theorem, it is possible to calculate the angle at which a camera from an unmanned platform can observe a protected object when flying at the maximum permissible

height. The minimum angle at which it can observe the object is 15 degrees, with the shorter the distance from the protected object boundary to the DRA-P zone boundary, the greater the angle of observation will be. For example, if the borders of the DRA-P zone are determined at a distance "L" of about 120 m, the angle of observation of the object from the platform will be equal to 45 degrees.

2. The boundaries of the DRA-P zone are at a distance "L" greater than 500 m from the boundaries of the protected object. According to the rules, the unmanned platform can perform a flight in the space between the 500th meter counted from the boundaries of the object and the border of the DRA-P zone. The flight can take place up to a height of 30 m above the ground. Using the Pythagorean theorem, it is possible to calculate the angle at which the camera from the unmanned platform can observe the protected object when the flight takes place at the maximum permissible height. The maximum angle at which it can observe the object is 15 degrees, with the greater the horizontal distance of the flying platform from the border of the protected object, the smaller the angle of observation will be. If there are any natural terrain obstacles, e.g. trees, between the protected object and the eye of the camera, it will be practically impossible to observe the object.

The decision to designate a DRA-P zone over a facility should be made after a thorough analysis of the actual threats and an assessment of the facility's vulnerability to attack using an unmanned aircraft. Only if the threat and vulnerability assessments indicate that the risks associated with a potential attack on the facility are unacceptable should the zone be designated. The designation of such a zone is a clear indicator that something important from the point of view of defence or national security is happening at a given facility.

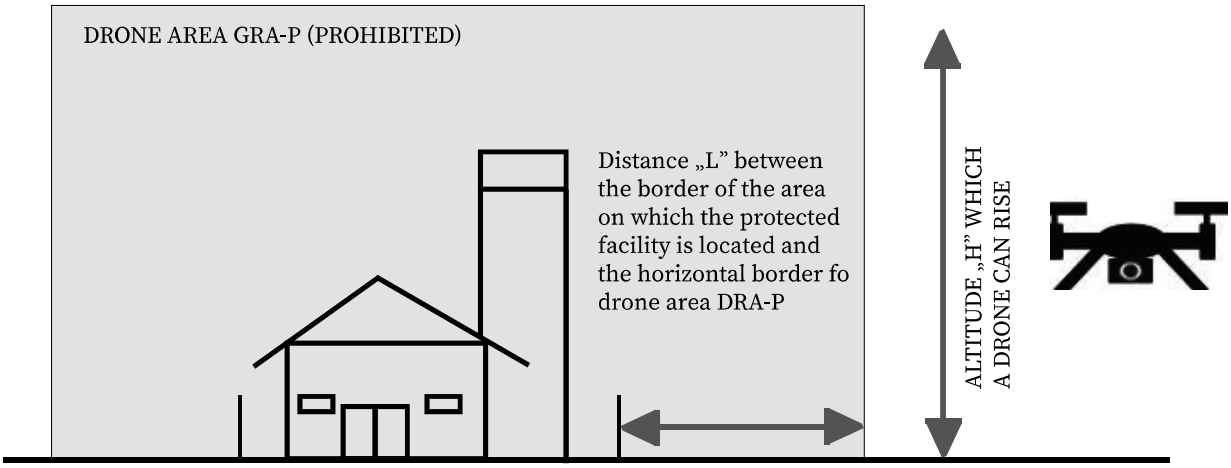

Fig. 5. Diagram of the DRA-P drone geographical zone.

Source: Author's own elaboration.

The use of devices to prevent flight into a protected space

Devices preventing the flight of unmanned aircraft include the Aeroscope[30]. However, it affects only DJI aircraft. It is not able to protect the protected object against aircraft manufactured by other companies or built by independent designers. Aeroscope can identify the aircraft's serial number, its location as read from the satellite signal receiver, its speed and direction of flight and the altitude at which it is flying. These parameters are read out in real time. Polish law does not require registration of the aircraft, which makes identification of the aircraft and assigning it to a particular pilot extremely difficult. The only possibility to identify the pilot is to declare the serial number of the aircraft, which each pilot must submit if he/she wants to fly in the aeronautical CTR zone, and to register the drone, i.e. to provide this number in the Pansa_UTM system[31]. Without this registration, it is not possible to obtain conditions for flight in CTR zones. However, if the aircraft was manufactured by a manufacturer other than DJI or by an independent builder, Aeroscope will not identify it. Aeroscope can also restrict a flight by designating a zone in which the flight will not take place. Such a function is called GeoFencing. The Aeroscope

[30] https://www.dji.com/pl/aeroscope [accessed: 30 XI 2021].

[31] https://utm.pansa.pl [accessed: 30 XI 2021].

operator can indicate the horizontal and vertical boundaries of the zone in which the flight cannot take place. DJI aircraft will therefore not be able to fly in this zone. The disadvantage of the device is that it cannot detect every DJI model and non-DJI models. An additional problem is posed by the storage of data collected by Aeroscope on the servers of the Chinese company DJI. This data can be used to obtain information about the location of protected facilities[32].

Training of police officers in aviation law, procedures in force in unmanned aviation and provisions allowing for punishment of pilots flying illegally

Such training should be a standard activity in Police units in whose area of operation there are objects important for the security or defence of the state. The training should cover European regulations:

- *Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation* (OJ EU L 212 of 22 VIII 2018, p. 1);
- *Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aerial systems and operators of unmanned aerial systems from third countries* (OJ EU L 152 of 11 VI 2019., p. 1);
- *Commission Delegated Regulation (EU) 2020/1058 of 27 April 2020 amending Delegated Regulation (EU) 2019/945 as regards the introduction of two new classes of unmanned aircraft systems* (OJ EU L 232 of 20 VII 2020., p. 1);
- *Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on rules and procedures for the operation of unmanned aerial vehicles* (OJ EU L 152 of 11 VI 2019, p. 45);
- *Commission Implementing Regulation (EU) 2020/639 of 12 May 2020 amending Implementing Regulation (EU) 2019/947 as regards standard scenarios for operations within visual range or beyond visual range* (OJ EU L 150 of 13 V 2020, p. 1).

The training should also cover the provisions of national law, including the *Aviation Law* Act and the guidelines of the President of the Civil Aviation Authority (ULC):

[32] https://www.911security.com/blog/dji-aeroscope-review-features-specs-and-how-its-used-in-layered-drone-detection [accessed: 30 XI 2021].

– *Guideline No. 7 of the President of the Civil Aviation Authority of 9 June 2021 on the modalities of operations using unmanned aircraft systems in relation to the entry into force of the provisions of Commission Implementing Regulation (EU) No 2019/947 of 24 May 2019 on rules and procedures for the operation of unmanned aerial vehicles* (Official Journal of the Civil Aviation Authority of 2021, item 35);
– *Guideline No. 24 of the President of the Civil Aviation Office of 30 December 2020 on the designation of geographical zones for unmanned aircraft systems* (Official Journal of the Civil Aviation Authority of 2020, item 78).

For facilities located in MCTR military zones, Police officers should also refer to the document:

– *Guidelines of the Commander-in-Chief of the Air Traffic Service of the Armed Forces of the Republic of Poland No. 6 of 17 September 2018 on detailing the principles of performing flights of flying models and unmanned aerial vehicles with an MTOW of 25 kg or less in air traffic zones of military airports (MATZ) and controlled zones of military airports (MCTR),* (https://ssrlszrp.wp.mil.pl/u/Wytyczne_w_sprawie_wykonywania_lotow_przez_RPAS.pdf).

In addition, Police officers should familiarise themselves with the use of the DroneRadar application used to image the structure of airspace, including the identification of horizontal boundaries of drone geographical zones. This application also allows to read the rules of performing flights by unmanned aerial vehicles in the zones. Knowledge of the law and familiarity with flight rules will allow police officers to identify pilots who perform flights in violation of flight rules.

The provisions allowing for the punishment of pilots flying against the rules are contained in various pieces of legislation. Selected provisions that talk about criminal liability are:

1. Within the scope of the *Act of 3 July 2002 Aviation Law* (i.e. Journal of Laws of 2020, item 1970, as amended):
   a) Article 211.1 Who:
      5) contrary to Article 97 of the Act, performs a flight or other aeronautical activities without a valid license or certificate of competence or contrary to their contents and conditions,
      6) contrary to Article 105, paragraph 2 of the Act, performs flights or other aerial activities despite the loss of the

required mental and physical fitness,

9a) contrary to Art. 123 par. 2, discharges from an aircraft in flight,

shall be subject to a fine, the penalty of limitation of liberty or deprivation of liberty for up to one year.

b) Art. 212.1. Whoever:

1. while performing a flight by means of an aircraft:

c) violates the air traffic regulations in force in the area where the flight takes place,

d) crosses the state border without the required permit or in breach of the conditions of the permit,

e) violates, issued pursuant to Art. 119 par. 2 of the Act, the prohibitions or restrictions on flights in Polish airspace introduced due to military necessity or public security

shall be subject to the penalty of deprivation of liberty for up to 5 years.

2. Within the scope of the Act of 6 June 1997 - Penal Code (Journal of Laws of 2021, item 2345, as amended):

a) Article 267.1. Whoever, without authorisation, gains access to information not intended for him by opening a closed letter, by connecting to a telecommunications network or by breaking or bypassing electronic, magnetic, IT or other specific protection thereof,

shall be subject to a fine, the penalty of limitation of liberty or deprivation of liberty for up to 2 years.

b) Art. 267.3. The same punishment shall be imposed on anyone who, in order to obtain information to which he is not entitled, sets up or uses a listening or visual device or any other device or software.

During the training, other regulations which have an impact on flight operations and are contained in legal acts should also be taught: Code of Petty Crimes, Atomic Law, Law on protection of persons and property, on protection of nature, on copyright and related rights, on protection of personal data. A police officer familiar with the above-mentioned regulations should know how to impede or prevent the flight of an unmanned aerial vehicle in the area of a protected facility.

Training of facility security staff in piloting multirotor and aerial vehicles

Facility security personnel should be competent to fly aircraft to enable them to effectively protect the protected facility. Aircrafts are capable of long-range flight over long distances. Aircraft equipped with cameras operating in the visible and infrared bands of electromagnetic waves allow observation of the foreground of the protected object both during the day and at night. Equipping these aircraft with a computer with installed software that uses AI algorithms to detect unusual activity should enable security personnel to prepare for an attack on the protected object. A multirotor aircraft allows for short distance flight, but can hover in one place. Such hovering allows for prolonged observation of a location where suspicious activity has been observed.

Masking the infrastructure of a protected facility

One of the ways of attacking facilities important to national security and defence is with cameras operating in the visible and infrared bands. The camera can be used to obtain information on the technology used at the facility, the technical equipment used in the physical protection system, the customs and procedures followed by the physical protection staff or other employees of the facility. Masking of infrastructure elements should prevent or hinder the acquisition of sensitive information from an unmanned platform.

Shielding of infrastructure elements from impact or from the effects of an explosive charge carried by the aircraft

An unmanned aircraft can be a useful platform for carrying explosive cargo or cargo containing chemicals. Explosive cargo can easily damage infrastructure components, causing the facility to slow down or stop operations. Contamination of the facility area or its foreground can have the same effect. The consequence of such an attack will be financial losses for the facility operator, financial losses for recipients of goods or services provided on the premises. Loss of health or life of employees of the attacked facility and losses related to environmental pollution are also possible. Shielding important parts of the facility's infrastructure

from the effects of an explosive device or from a direct hit by an unmanned aerial vehicle can protect the facility from the effects of an attack.

Measures for the benefit of the local community

Facilities that are important for the security or defence of the state are sometimes located in populated areas. Proper cooperation between the facility operator and the local population can help protect the facility. Local residents can easily recognise strangers behaving in an unusual way. Actions allowing to increase the degree of cooperation between the operator and the local population include: funding scholarships for talented young people, support for local health centres and hospitals, joint events such as "cleaning up the world", inviting local people to visit the protected facility in places where there are no devices sensitive from the point of view of protection of technological information or physical protection of the facility.

Conclusions

1. Paralysis of the functioning of the state, including disruption or interruption of critical infrastructure systems may occur not only by attacking well-protected facilities where electricity is generated, but also by attacking unprotected infrastructure used to deliver energy to the consumer,
2. The electricity grid in Poland is, with the exception of insulated lines, not resistant to short-circuit attacks using a cable suspended from an unmanned aerial vehicle.
3. Unmanned aerial vehicles, even the smallest ones, will easily lift a small payload of copper wire, which can be used to cause a short circuit.
4. The length of overhead lines and the multiplicity of substations serving them practically exclude any chance of preventing an attack by short circuiting the installation.
5. Successful attacks can result in large financial losses for both the power generator and grid operator and for power consumers.
6. Designs for new overhead lines must take into account the emergence of new sources of threat, which are drones. Thus, overhead

lines should, where possible, be built with insulated conductors in such a way that they cannot be short-circuited by a drone. An impulse to change the way lines are designed may be provided by the project of increasing the cabling of medium-voltage networks by 2040. Such cabling should be carried out as long as the level of network cabling in Poland does not equal the average EU level.

7. Properly designated DRA-P zone allows to increase the level of security of the protected facility. Due to the ease of attack, the designation of DRA-P zones around node points, critically important for the transmission of electricity in the country, should be considered.
8. The location of the DRA-P zones is public and information about it is available to everyone, so the selection of objects, for which the designation of DRA-P zones could be critically important, must be carried out with extreme caution.
9. In the absence of technical capabilities and given the financial constraints of network operators, it is worth considering preventive measures to secure facilities where electricity is generated and those used for the transmission of electricity by means other than detection devices and UAV neutralisation systems.

Bibliography

Baldick R., Chowdhury B., Dobson I., *Initial review of methods for cascading failure analysis in electric power transmission systems IEEE PES CAMS task force on understanding, prediction, mitigation and restoration of cascading failures*, w: *IEEE Power and Energy Society General Meeting – Conversion and Delivery of Electrical Energy in the 21st Century*, 2008.

Carter B., Mancini R. , *Op Amps for Everyone*, Burlington 2009.

Jaworski M., Szuba M., *Analiza obciążeń napowietrznych linii najwyższych napięć w aspekcie wytwarzania pola magnetycznego* (Eng. Load analysis of overhead high-voltage lines in terms of magnetic field generation), „Przegląd Elektrotechniczny" 2015, no. 5, pp. 149–154.

Kapoor R. et al., *UAV Navigation Using Signals of Opportunity in Urban Environments. An Overview of Existing Methods*, 1st International Conference on Energy and Power, ICEP2016, 14–16 XII 2016, Melbourne, Australia.

Metzger F.B., *An Assesment of Propeller Aircraft Noise Reduction Technology*, ASA Contractor Report 198237, 1995.

Parfomak P.W., *Physical Security of the U.S. Power Grid. High-Voltage Transformer Substations*, Congressional Research Service, 17 VI 2014.

Preece W.H., *On the Heating Effects of Electric Currents. No. II*, „Proceedings of the Royal Society of London" 1887–1888, vol. 43, no pagination.

Preece W.H., *On the Heating Effects of Electric Currents. No. II*, „Proceedings of the Royal Society of London" 1887 1888, vol. 44, no pagination.

Standardowe Specyfikacje Funkcjonalne. Elektroenergetyczna automatyka zabezpieczeniowa, pomiary i układy obwodów wtórnych (Eng. Standard Functional Specifications. Electricity protection control, metering and secondary circuits), Warszawa 2010 (update 2012).

Stauffacher E.R., *Short-time Current Carrying Capacity of Copper Wire*, „General Electric Review" 1928 r., vol. 31, no. 6, pp. 326–327.

Yuliang W. et al., *Noise Reduction of UAV Using Biomimetic Propellers with Varied Morphologies Leading-edge Serratio*n, „Journal of Bionic Engineering" 2020, vol. 17, pp. 767–779.

Internet sources

Energetyka, dystrybucja, przesył (Eng. Energy, distribution, transmission), PTPiREE, http://ptpiree.pl/raporty/2021/raport_ptpiree_2021.pdf [accessed: 30 XI 2021].

Legal acts

Commission Implementing Regulation (EU) 2020/639 of 12 May 2020 amending Implementing Regulation (EU) 2019/947 as regards standard scenarios for operations within visual range or beyond visual range (OJ EU L 150, 13 V 2020, p. 1).

Commission Delegated Regulation (EU) 2020/1058 of 27 April 2020 amending Delegated Regulation (EU) 2019/945 as regards the introduction of two new classes of unmanned aircraft systems (OJ EU L 232, 20 VII 2020, p. 1).

Commission Implementing Regulation (EU) 2020/746 of 4 June 2020 amending Implementing Regulation (EU) 2019/947 as regards the postponement of the dates of application of certain measures in relation to the COVID-19 pandemic (OJ EU L 176, 5 June 2020, p. 13).

Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on rules and procedures for the operation of unmanned aerial vehicles (OJ EU L 152 of 11 VI 2019, p. 45).

Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aerial systems and third-country operators of unmanned aerial systems (OJ EU L 152 of 11 VI 2019, p. 1).

Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Agency for Aviation Safety and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 of the European Parliament and of the Council 2014/30/EU and 2014/53/EU and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (OJ EU L 212 of 22 VIII 2018, p. 1).

Act of 3 July 2002 Aviation Law (i.e. Journal of Laws of 2020, item 1970, as amended).

Act of 6 June 1997 - Penal Code (i.e.: Journal of Laws of 2021, item 2345, as amended).

Guideline No. 7 of the President of the Civil Aviation Authority of 9 June 2021 on how to conduct operations using unmanned aircraft systems in connection with the entry into force of the provisions of Commission Implementing Regulation (EU) No 2019/947 of 24 May 2019 on rules and procedures for the operation of unmanned aircraft (Official Journal of the Civil Aviation Authority of 2021, item 35).

Guideline No. 24 of the President of the Civil Aviation Office of 30 December 2020 on the designation of geographical zones for unmanned aircraft systems (Official Journal of the Civil Aviation Office of 2020, item 78).

Guidelines of the Commander-in-Chief of the Air Traffic Service of the Armed Forces of the Republic of Poland No. 6 of 17 September 2018 on detailing the rules for flights of flying models and unmanned aerial vehicles with MTOW not exceeding 25 kg in air traffic zones of military airports (MATZ) and controlled zones of military airports (MCTR), https://ssrlszrp.wp.mil.pl/u/Wytyczne_w_sprawie_wykonywania_lotow_przez_RPAS.pdf.