SECURITY & DEFENCE QUARTERLY

https://securityanddefence.pl/

Proposed method for building an anti-drone system for the protection of facilities important for state security

Jędrzej Łukasiewicz[1], Anna Kobaszyńska - Twardowska[2]

[1]jedrzej.lukasiewicz@put.poznan.pl

https://orcid.org/0000-0002-7082-8511

[2]anna.kobaszynska-twardowska@put.poznan.pl

https://orcid.org/0000-0002-3087-8119

[1,2]Faculty of Civil Engineering and Transport, Poznań University of Technology, pl. Marii-Skłodowskiej Curie 5, 60-965 Poznań, Poland

Abstract

Unmanned aerial vehicles (UAVs) pose a threat to buildings and facilities important to the security of the state. As they are able to operate like individual aircraft, the number of ways they can be used for terrorist activity is practically unlimited. Anyone in charge of a facility that is crucial for the reliable functioning of a state is obliged to ensure an acceptable level of security. Since drones can be used to attack protected structures, they need to be protected by an anti-drone system. The paper proposes a method for assessing the effectiveness of systems for detecting and neutralising unmanned aerial vehicles. In order to suggest a new method for assessing the effectiveness of anti-drone systems, an analysis of the scientific literature and other documents describing existing anti-drone systems has been carried out. Attacks involving the use of drones, both in wartime and in incidents of terrorism, are also analysed and existing anti-drone solutions assessed. Because there are a variety of technical solutions for the detection and neutralisation of drones, and different location and weather conditions, a universal method is proposed based on probability calculations and neutralisation of drones, using mathematical formulas. This method allows for the effectiveness of the entire anti-drone system to be assessed on the basis of measuring the probability of detection and neutralisation of drones in real conditions. The proposed method allows the effectiveness of the currently existing anti-drone systems to be evaluated and for new methods for detecting and neutralising drones to be proposed. This method, based on mathematical calculations, enables software to be written for simulating anti-drone systems on computers and for the effectiveness of these systems to be confirmed before their construction in a protected facility.

Keywords:

unmanned aerial vehicle, probability of detection, probability of neutralization, anti-drone prevention, critical infrastructure

Article info

Received: 20 February 2022
Revised: 1 April 2022
Accepted: 18 April 2022
Available online: 9 June 2022

Citation: Łukasiewicz, J. and Kobaszyńska - Twardowska, A. (2022) 'Proposed method for building an anti-drone system for the protection of facilities important for state security', Security and Defence Quarterly, 39(3), pp. 88–107. doi: 10.35467/sdq/149268.

Introduction

Unmanned aerial vehicles are aircraft that can carry out flight missions autonomously or by remote control from the ground, without the presence of a pilot on board. There are several types of unmanned aerial vehicles, including: multirotors, planes, helicopters, hybrid ships, including planes capable of vertical take-off (Singhal *et al.*, 2018). These vehicles can be of various sizes and weights. In general, unmanned aerial vehicles, because of their diverse structure, are considered as universal flying platforms, allowing various types of missions in different weather and location conditions to be carried out. Pursuant to European regulations, unmanned aerial vehicles must be certified and, as a result of certification, receive the vehicle's class designation (Commission Delegated Regulation, 2019). A vehicle's class is a set of technical requirements that must be met by an unmanned aircraft for a given class. C0, C1, C2, C3, C4, C5 and C6. Class C5 and C6 are classes of aircraft used for the transport of people and dangerous goods. The remaining classes include vehicles that have different take-off masses, but not exceeding 25 kg. Unlimited access to parts means that it is possible to build a custom drone, whose flight characteristics will only depend on the constructor's fantasy. Building a drone is a relatively uncomplicated process and does not require deep technical knowledge. The cost of the components needed to build a drone is significantly lower than the price of a finished, commercially manufactured drone. The drone can therefore be a used as a weapon by people or groups with limited financial resources. Table 1 contains the characteristics, defined by law, which can be used for drone detection.

A comparison of the size and reflection area of the radar beam of some currently manufactured multirotors is shown in Figure 1. The dimensions are as follows: DJI Mavic Mini 2 – 159×203×56 mm, DJI Phantom 4 – 290x290x196 mm, DJI Matrice 200 – 887×880×378 mm.

Because they can operate without a pilot on board for many kilometres and can carry cargo, unmanned aerial vehicles can be used in terrorist attacks on people and structures important for state security, including critical infrastructure. Drone attacks are reported in the media every day.

On January 17, 2022, fuel tanks at installations in Abu Dhabi were attacked and two people were killed (Aljazeera, 2022). A famous drone attack was the Greenpeace attack on the Bugey nuclear installations in France (Pradier, 2018). The attack consisted in smashing a drone, whose shape was unusual and resembled the silhouette of Superman, against a concrete building containing a nuclear reactor. Hitting the reactor's cover itself did not cause any damage to people and installations but the media heavily criticised the plant operator and emphasised that the facility was unprepared. Greenpeace put forward arguments that the power plant would be a source of environmental contamination in the case of a successful attack.

Drones pose a threat to structures and people. Operators of facilities important for state security, including operators of critical infrastructure (CI) facilities, must install effective drone detection and neutralisation systems.

The study aims to show how detection and neutralisation systems for unmanned aerial vehicles are built, based on the probability of detection and neutralisation of drones by these systems' devices. Applying the proposed method may contribute to increasing the effectiveness of detection and neutralisation systems and therefore increase the level of security of facilities protected by these systems.

Figure 1. Comparison of the size and reflection area of the radar beam of A – DJI Mavic Mini 2, B – DJI Phantom 4 and C – DJI Matrice 200 (DJI, 2022a,b).

	CLASS				
Requirements	**C0**	**C1**	**C2**	**C3**	**C4**
Maximum take-off mass or kinetic energy at the moment of impact	250[g]	900[g] / 80[J]	4[kg]	25[kg]	25[kg]
UAV maximum size	no limits	no limits	no limits	3[m]	no limits
Maximum velocity	19[m/s]	19[m/s]	no limits	no limits	no limits
Power supply	electricity	electricity	electricity	electricity	no requirements
Communication frequencies	no frequency requirements	no frequency requirements	no frequency requirements	no frequency requirements	no frequency requirements
Additional requirements	no requirements	in the event of an interruption of the control and monitoring link, it must have a predictable method of restoring the command and control link or terminating the flight	in the event of an interruption of the control and monitoring link, it must have a predictable method of restoring the command and control link or terminating the flight	in the event of an interruption of the control and monitoring link, it must have a predictable method of restoring the command and control link or terminating the flight	no requirements
Guaranteed sound power level	no requirements	not higher than 85dB and described on the label. Does not apply to fixed wing	not higher than 85dB and described on the label. Does not apply to fixed wing	must be guaranteed and described on the label	no requirements
If UAV is equipped with a remote network identification, system	no requirements	allows real-time transmission, from UAV, data e.g., flight location, velocity, etc.	allows real-time transmission, from UAV, data e.g. UAV serial number, flight location, velocity, etc.	allows real-time transmission, from UAV, data e.g. UAV serial number, flight location, velocity, etc.	no requirements

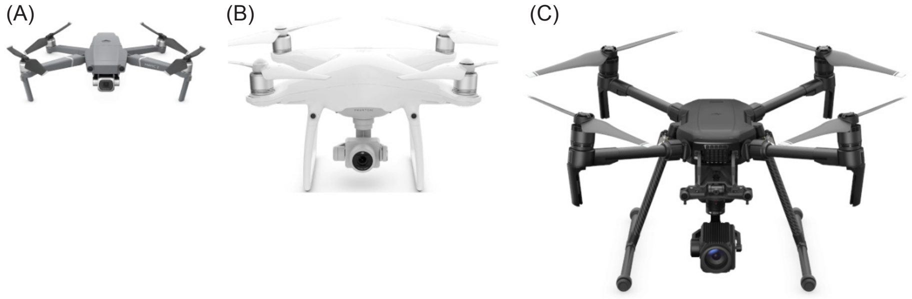


Table 1. Characteristics of UAVs that may have an impact on the effectiveness of detection and neutralisation (Commission Delegated Regulation (EU), 2019).

Drone attack methods

An unmanned aerial vehicle is a universal platform that can attack a target from different heights, with different speeds, on different flight trajectories and with different on-board equipment.

An unmanned aerial vehicle can be used to carry an explosive device (Grisaro *et al.*, 2021). The explosion of an explosive device affects the attacked object through a sharp change in pressure, emission of infrared radiation, i.e. heat, a seismic wave, if the explosion occurs close to the ground, and an acoustic wave, i.e. noise.

Detonation of the payload carried by a drone during an attack on people can result in death, serious injury or panic if it is an attack on a crowd of people. The most serious attack using a drone carrying explosives was the attack carried out on August 4, 2018 in Venezuela, in the city of Caracas, during which the president of the country, Nicolas Maduro was attacked (BBC News, 2018). The drones carried explosives that exploded, causing panic among the participants of a meeting, as well as injuring seven people. Another attack of this type was carried out in November 2021 on the Prime Minister of Iraq Mustafa al-Kadhimi (BBC News, 2021). The attack destroyed a house in the centre of a well-guarded district, the so-called Green Zone. Nothing happened to the prime minister, but the house that was attacked was badly damaged. Drone bomb attacks were carried out on September 14, 2019 on Aramco's oil installations in Saudi Arabia. As a result, the installations were burnt and were closed for repair. The attack resulted in the reduction of oil production by half and turmoil on global oil markets (BBC News, 2019). Aircraft mass produced by the world's leading manufacturers can be used for attacks (Monnik, 2021) and one example was the drones manufactured by one of the best producers in the world (Kasteloo, 2020).

Drones can be used to damage an object by physically hitting or transporting a device or element that will damage the target. An example of an attack carried out in this way is the attack that unknown perpetrators carried out in 2021 on the power grid in Pennsylvania, USA. The attack was to consist of a raid on the electrical system with a drone with a suspended electric wire in order to cause a short circuit, and thus turn off the power supply for large areas of the country (Hambling, 2021).

Unmanned aerial vehicles can be used to observe facilities important for state security. Currently produced vehicles are usually equipped with cameras. These cameras mean long distance observation can be achieved. They are equipped with an autofocus system and optics of the highest quality, allowing for high-quality image recording**.** Cameras operating in the visible light range can be supplemented with infrared sensors**.** Such a camera allows an image to be recorded in a situation of visible light deficit. It also allows the identification of system components. It is possible that cameras were used during the

Figure 2. Drone Swarm. Picture taken during Guinness world record breaking in China (Guinness World, 2021).

recent drone flights over Swedish nuclear installations. In January 2022, drone flights over nuclear power plants were observed in Sweden. Unauthorised flights were carried out over the installations of the Forsmark Nuclear Water Plant, Ringhals and Oskarshamn Nuclear Power Plants (BBC News, 2022). These flights did not result in losses of people or installations, but their purpose may have been to gather intelligence. Forsmark Power Station is the largest electricity producer in Sweden (Reuters, 2022). The cameras make it possible to observe people and obtain data on the technologies used in the observed facility, the topography of the observed facility and so on. The use of drones to wiretap personnel radio communication, including Internet communication, is also possible.

The examples given of drone attacks above do not cover all possible scenarios of their use. Due to the different properties of drones resulting from their construction, taking into account that the drone pilot may have worse or better training, and because of the development of unmanned aerial vehicle technology, it should be assumed that there are significantly more ways to attack. A problem that is mentioned increasingly often is the use of a swarm of drones, in military and terrorist applications, in a simultaneous attack on a target. Previous reports suggest the possibility of using a swarm of drones for civilian purposes (Tahir *et al.*, 2019), but there is no doubt that swarm technology will sooner or later be used in a terrorist attack. The current record for a simultaneous flight of a swarm of drones is 3281 pieces (Guinness World, 2021).

To date, not a single attack carried out by a swarm of drones on facilities important for the security of the state has been recorded.

How to prevent drone attacks is described in (Abdalla *et al.*, 2020; Ziyang *et al.*, 2018). A description of drones as a real threat features in Drone Attacks Against Critical Infrastructure (Crino and Dreby, 2020).

Drone detection methods

The current drone detection systems, which are elements of anti-drone systems that protect facilities, operate using various features of unmanned aerial vehicles (Yaacoub *et al.*, 2020). The characteristics of unmanned aerial vehicles that can be detected include heat emitted by the aircraft, noise emitted by propellers and motors and that resulting from the flow of the vehicle by air jets, the shape of the aircraft and electromagnetic radiation of various frequencies emitted by communication systems operating during flight. Drones can also be detected by radar.

Detection of heat emitted by an aircraft is achieved by cameras operating in the infrared band of electromagnetic radiation (Andraši *et al.*, 2017). The source of heat on the unmanned aerial vehicle could be a lithium-polymer battery which is a source of electricity, rotating engines and electronic speed controller system designed to regulate the speed of rotation of the engines. Other electronic systems, including the on-board computer, do not emit large amounts of heat. It is possible to detect an object at a temperature other than that of the surrounding air space. However, it is possible to design the drone in such a way that the heat emitted by it is dissipated. Methods for dissipating heat in airplanes are known from manned aviation. In the case of unmanned aircrafts, heat dissipation is achieved by attaching sinks to heating elements of heat or by mounting heating elements in air jets.

Aircraft sound is detected using microphones (Schäffer *et al.*, 2021). However, detecting an aircraft with a microphone is relatively difficult. The aircraft may be constructed so that the propeller rotation speed is low. The rotation speed can be reduced by using larger diameter propellers. In this case, little noise is emitted by the propeller. Another method for reducing the sound level may be to perform a gliding flight. Additionally, the drone's sound may be muffled by noise emitted by the surroundings of the detection system. If the protected facility is in an inhabited area, the sound source may be public transport, cars, sounds from nearby industrial plants, and the noise of planes landing in the city. *T*he detection efficiency of the drone's acoustic signal could be improved by using microphone arrays (Beamforming algorithms, 2016; Burshtein and Weinstein, 2001; Gannot *et al.*, 2001). Intensity of sound is defined as the sound power per unit area. Intensity is inversely proportional to the square of the distance (Abdullah *et al.*, 2019):

$$I(r) \sim 1/r^2 \qquad (1)$$

Where I is intensity of the sound and r – is distance from the source of the sound.

It means that the intensity of the sound emitted by the drone, which can be registered by the microphone of the physical protection system, will decrease with the square of the distance from the drone and it could be very difficult or impossible to detect this sound from a long distance away.

The aircraft can be detected using vision methods (Hirabayashi *et al.*, 2020). Good weather conditions are a prerequisite for detection. Night, fog, and precipitation all reduce the effectiveness of the cameras. The camera can observe a flying object, but observation itself is not easy. A plane flying at a distance of 1000 metres with a wingspan of 2 metres is a spot with a cone of observation of 0.12 DEG. The observation cone for a drone flying closer will have a greater viewing angle, and the image itself will be recorded by a greater number of pixels. This is the reason for the use of variable focal length lenses in optical detection. The image of a multirotor flying at a distance of 1000 metres is even smaller, which makes it more difficult to detect and resembles a point in the sky. Observation alone is not enough. The image analysis system must identify what kind of object has been observed. The observed object could be a bird. The image analysis system, using artificial intelligence technology, can identify the drone on the basis of learned algorithms (Wu et al., 2017). The disadvantage of this system is the difficulty in teaching the system to recognise an object correctly. Such teaching is a long and difficult process and requires thousands of photos (Barisic *et al.*, 2019). Additionally, if the attacker knows the rules of detection, he can build a drone with an unusual shape, such as the above-mentioned Superman, or in the shape of a bird. In the event of an attack with such a drone, the image recognition system will be cheated.

Detection of an unmanned aerial vehicle is possible by detecting communication between a flying aircraft and a ground station (Al-Sa'd *et al.*, 2019). For communication, electromagnetic radiation with different oscillation frequencies is used. Currently, the most popular frequencies used to control drones are 2.4GHz, 5.8GHz, 433MHz and 868Mhz (Oh *et al.*, 2020). Increasingly, communication between the UAV and the ground station can be maintained via GSM communication (Solidakis, 2017). The method for detecting communication, however, is an unreliable, inefficient method. One of the reasons for the low detection efficiency is the ability to perform an unmanned mission without the need to communicate with the ground station during the flight. When planning a mission, the pilot can use software in which he marks the points to which the aircraft is to fly (the so-called waypoints) on a map and, in more advanced systems, he can indicate what the aircraft is to perform at a given point e.g. a vehicle can drop a cargo and take a photo. Applications for controlling mass-produced drones by leading manufacturers are delivered with the drone to the buyer. In the case of self-built systems, applications, usually open-source, can be copied from the Internet at no extra charge. If, during the flight, the drone sends messages to the ground station, this communication can be detected by the electromagnetic radiation detector and the anti-drone system can take neutralisation measures. The multitude of frequencies at which communication takes place, as well as the possibility of using non-standard frequencies, is the reason why detection is difficult. The detection device must scan the entire frequency spectrum of electromagnetic radiation and decide which frequencies are used for drone and ground station communication and which are for other purposes. There are communication detection devices for specific models on the market. One such device is the DJI AeroScope (DJI), which in the stationary version detects communication between the drone and the pilot at a distance of up to 50 km, while in a portable version at a distance of up to 5 km. The intensity of the radio signal decreases with the square of the distance and is described similarly as in the case of sound by the equation (1). It is also possible to detect communication between the drone and the pilot using Software Defined Radio (SDR) devices (Ferreira *et al.*, 2022). These devices are notably cheap. Because they can be programmed, such devices can integrate the functions of detection, locating, jamming and spoofing of the GPS signal.

The last method for detecting a drone is the radar detection method (Park *et al.*, 2021). Radar devices can detect drones flying at high altitudes and at a long distance from the protected facility. Detection of drones is carried out with the help of radar operating at different frequencies (Ochodnický *et al.*, 2017; Quevedo *et al.*, 2018). The construction of radar devices also uses techniques that increase the effectiveness of object detection, such as beamforming (Maestre *et al.*, 2019). The effectiveness of radar systems increases as the distance between the drone and the radar antenna decreases (Ezuma *et al.*, 2021; Radartutorial). The radar signal to noise ratio then increases.

Radar devices are commonly used, although their effectiveness strongly depends on the location of the protected facility. Drones can perform missions at very low altitudes. They are equipped with flight altitude measuring devices, including barometer, ultrasound sensor or lidar, and can even fly at altitudes of about 50 cm above the ground. Low flight over uneven, bumpy terrain is the reason why the radar will not detect the aircraft. The drone will also not be detected if the area surrounding the protected facility is overgrown with bushes or trees.

Drone neutralisation methods

The existing methods for neutralising drones are not fully effective Therefore, neutralisation systems consist of devices whose operation is based on different principles.

One of the methods of neutralising a drone is destroying it with laser light (Rafael). The high-energy light beam may cause the drone to fall after being hit. These systems are effective in good weather conditions. In fog or precipitation, the laser light is scattered on the water molecules. The laser device is placed on the gimbal so it can point in any direction. Unfortunately, a drone neutralised by this method falls to the ground in an uncontrolled manner. A drone fall could have serious consequences. It could fall on people and on sensitive elements of the installations of the protected facility. A drone is usually seriously damaged when it falls, so the data stored on its computer will be unreadable. This will make it impossible to identify the pilot and bring him to justice.

Another method of neutralisation is to catch a drone in a net (Droptec). Such a net can be launched from a netgun operated on the ground by the facility security personnel, but it can also be fired from a netgun hung over another unmanned aerial vehicle piloted by a member of the facility security personnel. This method is effective when a shot is fired at close range, which can be up to 30 metres. A drone caught in a net, to which a parachute can be attached, descends at a low speed, meaning it is not damaged when it hits the ground. Data from the computer of a drone captured in this way can be read and the pilot identified.

Another way to neutralise a drone is to damage its electronics with an electromagnetic pulse (National Interest, 2021). A high-energy electromagnetic pulse can damage the drone's electronic components such as its computer or electronics speed controller systems that control the speed of rotation of the engines. The range of this type of impulse can be several kilometres. This type of weapon can damage a typical drone. A constructor who knows the influence of an electromagnetic field on electronics can isolate it from the influence of an external electromagnetic field by using the so-called Faraday shield (Krauss, 1992)**.** In addition, filters are placed on the electric wires in the drone's housing, whose task is to cut off the high-intensity current pulse induced by the electromagnetic field from the anti-drone systems. The electromagnetic pulse emitted by the anti-drone device may affect other electronic devices, including those used to control technological processes in the protected facility.

Communication signal jamming devices between an aircraft and a ground station emit electromagnetic radiation at different frequencies, which include the frequencies used by an unmanned aerial vehicle. Communication between drone and ground station is disturbed by the emission of an electromagnetic wave with a flat spectrum and the noise intensity uniform for all emitted frequencies. If the interfering signal is emitted with sufficient power, the pilot loses the ability to control the aircraft. The communication disrupting device will be ineffective if the pilot programmes the drone prior to take off enabling it to carry out the mission in a completely autonomous mode.

A frequently used method for neutralising a flying aircraft is to distort the signal of the satellite positioning system (jamming) or spoof the system (spoofing) (Sahmoudi and Amin, 2009). The disturbance is that a signal is emitted from the interfering device at the frequencies at which the positioning system works. The interfering signal is more powerful than the satellite signal. The satellite receiver on board the unmanned aerial vehicle is confused by the jamming device and is not able to correctly determine its position. Spoofing is where a spoofing device emits a signal containing a falsified position. The aircraft assesses its position on the basis of a false signal and it will fly to the place indicated by the device pointing at the wrong position instead of to the target and the attack will be ineffective. The answer to this method of defence may be navigation, which allows the position of the aircraft to be determined in the absence of access to the signal of the positioning system. Navigation systems, in conditions of lack of access to a satellite signal, identify the position of the aircraft from the lidar reading, ultrasonic distance measuring devices, camera systems operating in the visible or infrared field (He *et al.*, 2018). Another method of navigation without the use of a satellite positioning system is the deployment of ground stations emitting the position signal and navigation based on triangulation (Kapoor *et al.*, 2017).

The low efficiency of the currently used neutralisation systems makes it necessary to look for other, new solutions. One of the recently proposed methods is to disrupt the flight of the drone by cheating the algorithms of analysing the image recorded by the drone's camera (Zhou *et al.*, 2021). This method takes advantage of the weakness in which the image analysis algorithm miscalculates the drone's distance from the obstacle as a result of camera illumination from two different light sources. By controlling the light intensity, one can make the algorithm detect an obstacle and stop the drone's flight.

Proposed method for building a drone detection system

The drone detection systems currently being produced are not sufficiently effective to detect a flying drone. Such systems should therefore be based on devices operating on different principles. Detection devices in physical protection systems are selected by assessing the probability of detecting unwanted activity in given conditions. Drone detection systems consisting of devices operating on different principles should also be built based on the probability of detecting a drone in given conditions.

For each detection device, the probability of detection under given operating conditions and in the required time period should be experimentally assessed. The given operating conditions of the device are the conditions in which the device will operate. Therefore, the probability of drone detection is assessed for:

- different weather conditions (WC) (humidity, fog, rain, snow, no precipitation, high temperature, low temperature, no wind, strong wind, high noise environment, low noise environment etc.),
- at any time of day or night (t),
- detection in a given location of a protected facility (L) (flat, mountainous area, area covered with bushes, forest, built-up area, undeveloped area etc.),
- various types of unmanned aerial vehicles (T) (multirotor, plane, helicopter, ship with an unusual shape),
- various types of motor (M) (electric, combustion engine),
- use with various methods for performing the aircraft's mission (PAM) (high altitude flight, low-level flight, high-speed flight, low-speed flight, straight-line flight, flight on a diversified trajectory),
- use with different competences of the physical security personnel responsible for operating detection devices (C) (well-trained employee, employee without experience),
- use over different distances (D) between the flying UAV and detection device (long distance, short distance).

The detection probability assessment can be performed by counting the number of detections of the flying drone per hundred flights. When there are one hundred detections out of one hundred drone flights under the given conditions, the probability will be 100% and if not a single flight is detected, the probability will be 0%. An additional parameter to be assessed must be the detection time, known as the required time. The required time is the time when a drone is detected early enough to activate any planned procedures in the event of a drone attack. One such procedure could be to activate the drone's neutralising devices and direct them towards the attacking drone.

The probability of drone detection in given conditions and in the required time is marked as P_{ux}, with the ux index being the x detection device.

The total probability of the drone being detected by a system made of N devices is given by the formula:

$$P_{totalD} = 1 - (1 - P_{u1})(1 - P_{u2})...(1 - P_{uN}) \tag{2}$$

where $P_{ux} = P_{ux}(WC, t, L, T, M, PAM, C, D)$;

Example 1:
Let's assume that one is building a drone detection system composed of three detection devices. In the described example, in which the detection system consists of three devices, one has three probabilities P_{u1}, P_{u2} and P_{u3} after the tests. For the described system, the formula takes the form:

$$P_{totalD} = 1 - (1 - P_{u1})(1 - P_{u2})(1 - P_{u3}) \tag{3}$$

Let us consider a system consisting of three detection devices, the detection probability of which determined for given conditions and in the required time is, respectively, $P_{u1} = 0.33$, $P_{u2} = 0.65$, $P_{u3} = 0.54$. This means that for one hundred flights, these devices detected the drone, respectively, u1 → 33 times, u2 → 65 times, u3 → 54 times. The calculated total probability of a system detecting the drone will therefore be equal to:

$$P_{totalD} = 1 - (1 - 0.33)(1 - 0.65)(1 - 0.54)$$

$$P_{totalD} = 0.89 \text{ or in other words } P_{totalD} = 89\%$$

This result suggests that a system composed of P_{u1}, P_{u2} and P_{u3} detects the UAV with a probability of 89%, so out of a hundred flights, it detects 89 flights. If the object were protected by such a system, eleven out of every hundred passes would not be detected and it could successfully launch the attack.

The task of the manager of the protected facility is to determine the minimum threshold value P_{totalD} below which the system is considered ineffective. If the system is deemed ineffective, steps should be taken to increase the value of P_{totalD}. This can be achieved by:

- change of detection conditions, e.g. when the device does not cope well in an open area covered with bushes, you can cut bushes,

- increasing the number of detection devices in the system, assuming that subsequent devices operate on a different principle than those already used to build the system,

- changing the device with the lowest detection probability for the better, or

- if there is no better device model on the market, preventive actions described later in this article should be taken in order to prevent the launch of an attack.

Example 2:
Let's assume that the drone detection system described above does not meet the expectations and that the total probability of system detection should be higher. The detection system constructor can increase the probability of detection by adding other detection devices to the system that operate on a different principle than those already working in the system. Additional devices with the probability of drone detection in the given conditions and in the required time can therefore be provided, respectively $P_{u4} = 0.50$ and $P_{u5} = 0.60$. Thus, the considered system consists of five detection devices. The calculated total probability of detecting the drone by such a system is equal to:

$$P_{totalD} = 1 - (1 - P_{u1})(1 - P_{u2})(1 - P_{u3})(1 - P_{u4})(1 - P_{u5}) \quad (4)$$

$$P_{totalD} = 1 - (1 - 0.33)(1 - 0.65)(1 - 0.54)(1 - 0.5)(1 - 0.60)$$

$$P_{totalD} = 0.98 \text{ or in other words } P_{totalD} = 98\%$$

This result indicates that the system with an unacceptable probability of drone detection, after supplementing it with other detection devices, is very effective, and the total probability of detection increases by about 10% to 98%. If the facility were protected by such a system, only two out of every hundred flights would be undetected and the attack will be successful.

When examining detection devices, security personnel should remember a few principles that determine the effectiveness (and thus the probability) of detection:

- detection devices must be absolutely independent of each other. Independence means that these devices must have different, separate power sources, they must have different, separate protection against interruption of operation, and the detection devices must not influence each other in any way, e.g. by disturbing their operation through a strong electromagnetic field,

- the detection equipment and the entire detection system must be inspected periodically. Periodic inspection results from the fact that each technical object may be damaged, which will result in a radical decrease in the value of P_{totalD}, maybe even below the permissible threshold value. The control is also due to the fact that every technical object is getting old. The detection system should also be tested whenever the system operating conditions change. Such a change may be e.g. the construction of buildings or structures in the area of the protected facility.

- the priority for the manager of the protected facility should be to ensure effective detection of the attacking drone, and not the cost of building the system.

The drone detection system is considered to be properly constructed if the value of P_{totalD} is higher than the permitted minimum threshold value.

When designing a drone detection system for the protected facility, the detection devices should be selected in such a way that their operation does not adversely affect the operation of other devices used in the protected facility. Such negative influence may include, for example, the electromagnetic field emitted by the radar. If such a field, its frequency and intensity, would interfere in any way with the operation of the protected object, then such a detection device should be abandoned or measures reducing the influence of the electromagnetic field on the devices in the protected object should be applied, e.g. by means of appropriate shielding.

Proposed method for building a drone neutralisation system

The devices for neutralising drones currently available on the market do not provide effective protection of the facility. The drone neutralisation system should therefore be built of drone neutralisation devices in different ways so that the probability of neutralisation is high enough. The use of devices operating on different principles ensures that the system will fulfil its task in all conditions, i.e. neutralise the drone. The drone neutralising devices should be selected for the system after assessing their effectiveness, i.e. the probability of neutralising the drone in the given conditions and in the required time. The assessment of the probability of drone neutralisation should take place in the same conditions as the drone detection devices are assessed. The effectiveness of neutralisation should be assessed:

- with regard to weather conditions (WC) (air transparency, wind strength, etc.),
- at any time of day or night (t),
- with regard to location conditions (L) (undulating terrain, height of vegetation in the vicinity of the defended object, buildings, population of the area),
- with regard to aircraft type (T) (multirotor, plane, helicopter, ship with unusual shape),
- for various types of motor (M) (electric, combustion engine),
- sing different methods of attack implementation (PAM) (high or low flight altitude, flight at different speeds, flight on different trajectories, etc.),
- with regard to the competence of the physical security personnel responsible for operating the system (C),
- for various distances (D) between flying UAV and detection device (long distance, short distance).

The assessment of the probability of neutralising the drone of each neutralising device can be performed by counting the number of effective actions as a result of which the drone ceases to pose a threat to the protected object per one hundred attempts. An additional parameter to be assessed should be the time required for the effective neutralisation of the drone. The time required is the time when the drone is neutralised quickly enough to be unable to successfully end an attack e.g. fast enough that the drone fails to transport the explosive close enough to the target that its explosion causes losses, or fast enough that the drone cannot record the image for an intelligence mission.

The probability of the device neutralising the drone is denoted by the P_{uy} symbol, while the index uy is the symbol of the y-neutralising device. The total probability of the drone being neutralised by a system composed of N devices is given by the formula:

$$P_{totalN} = 1 - (1 - P_{u1})(1 - P_{u2})...(1 - P_{uN}) \quad (5)$$

where $P_{uy} = P_{uy}(WC, t, L, T, M, PAM, C, D)$;

Example 1:
Consider a situation where an attacking drone has been detected and the system consists of three neutralising devices. The probability of neutralising the drone determined for the given conditions and in the required time is equal, respectively, to: $P_{u1} = 0.5$, $P_{u2} = 0.65$, $P_{u3} = 0.64$. This means that these devices neutralised the drone one hundred times: u1 → 50 times, u2 → 65 times, u3 → 64 times. Thus, the calculated total probability of the drone neutralisation by such a system is equal to:

$$P_{totalN} = 1 - (1 - 0.5)(1 - 0.65)(1 - 0.64)$$

$$P_{totalN} = 0.94 \text{ or in other words } P_{totalN} = 94\%$$

This result indicates that a system composed of the P_{u1}, P_{u2} and P_{u3} devices neutralises the UAV with a 94% probability, so it neutralises approximately 94 flights per 100 passes.

If security personnel want to determine the probability of the drone being neutralised by the device, a few rules that determine the effectiveness (and thus the probability) of neutralization should be applied:

- The neutralisation facilities must be absolutely independent of each other. Independence means that these devices must have different, separate power sources, they must have different, separate protection against interruption of operation, and these devices must not have any influence on each other, e.g. by disturbing their operation through strong electromagnetic fields.

- The neutralisation devices, as well as the entire neutralisation system, must be inspected periodically. Periodic control results from the fact that each technical object may be damaged, which will result in a radical reduction of the P_{totalN} value, maybe even below the permissible threshold value. The control is also due to the fact that every technical object is getting old. The neutralisation system should also be tested whenever there is a change in system operating conditions. Such a change might be the construction of buildings or structures in the area of the protected facility.

- The priority for the manager of the protected facility should ensure effective neutralisation of the attacking drone, and not the costs of building the system.

The drone neutralisation system is considered to be properly constructed if the P_{totalN} value is higher than the permitted minimum threshold value.

When designing a drone neutralisation system for a protected facility, neutralising devices should be selected in such a way that their work does not adversely affect the facility or people working in its vicinity. Such a negative impact may include, for example, a drone fall as a result of shooting down an object or people with a laser device. The kinetic energy of a falling drone is described by the formula:

$$E_K = 1/2mv^2 \tag{6}$$

where: m – is the mass of the drone, v – the speed at which the drone hits the obstacle. The consequence of the fall of the drone, even with low kinetic energy, could be human injury or death, and if it hits a technical object, its operation may be interrupted. If the risk related to the fall of the drone onto installations or people would be unacceptable, reduction measures should be applied, e.g. by constructing covers.

The total success probability of the entire anti-drone system consisting of the detection system and the neutralisation system is given by the formula:

$$P_{total} = P_{totalD} \text{ x } P_{totalN} \tag{7}$$

The P_{totalD} and P_{totalN} values, as described above, are in the range (0–100%). The product of these two values will not be greater than the smaller value of the probability components, therefore

$$P_{total} < \min\{P_{totalD}, P_{totalN}\} \tag{8}$$

Recommendations for assessing the probability of detection and neutralisation of devices used in the construction of anti-drone systems

The effectiveness of the described method depends on the use of correct probability values for detection and neutralization of devices used in the construction of anti-drone systems. Both the probability of detection and the probability of neutralisation should be determined experimentally in order to prove the correctness of the parameters of the tested devices. The correct probability value can be obtained:

- by means of tests carried out by the manufacturer of the device or system,
- by means of tests carried out by the security personnel of the protected facility, who, when building the anti-drone system, must meet the requirements of obtaining at least the threshold probability of detection and neutralisation of the drone, and
- through tests carried out by a state institution specially appointed for this purpose, which should determine its effectiveness in an objective manner, independent of the manufacturer of the tested equipment.

The reliability of the technical objects which the proposed detection system consists of at the beginning of its use can be obtained from the manufacturer. The significance level should be up to 5%. Nevertheless, within time, in order to estimate the reliability of objects, non-reliability tests should be carried out on a representative sample. The sampling method has two elements: a sampling scheme (e.g. equal probability, probability proportional to size) and a forecasting (estimation) procedure. Together, these two elements provide the framework for calculating the population abundance. The use of a statistical method is recommended. Statistical sampling methods allow the selection of a sample that is representative for the population. The ultimate goal is to forecast (extrapolate or estimate) the value of a parameter ("variable") observed in the sample for the population, which allows to determine if the population contains significant irregularities and, if so, what their extent is. Sample size n is calculated based on the following information:

- population abundance,
- confidence level determined from the normal distribution,
- maximum allowable error (usually 5%),

- expected error selected by the operator in accordance with his professional judgment, and on the basis of information from previous tests,

- standard deviation of errors.

The sample size is calculated as follows (European Commission, 2017):

$$n = \frac{Nu^2\sigma^2}{N\Delta^2 + u^2\sigma^2} \tag{9}$$

where:
N – population abundance,
u – value for the specified significance level,
σ – standard deviation,
Δ – limit deviation.

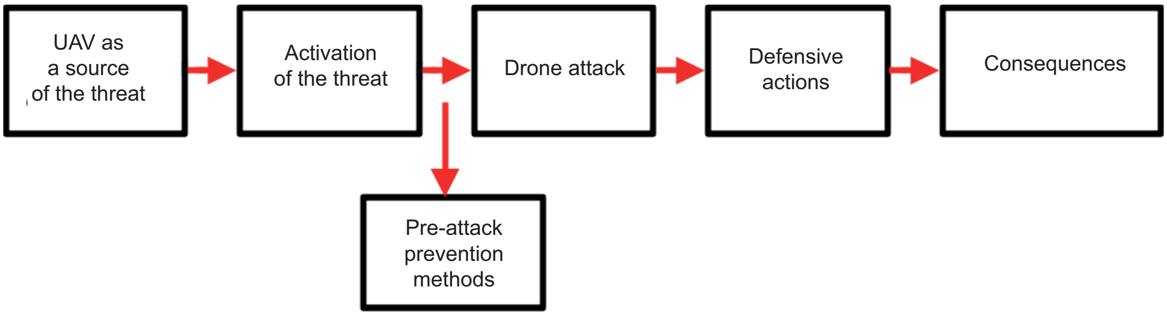
The appointment of a state institution for testing should contribute to the standardization of requirements for anti-drone devices and to ensure that the effectiveness of the anti-drone system, not its price, is the priority.

The assessment of the probability of detection and neutralisation of anti-drone systems makes it possible to check whether a given system is effective and whether it meets the requirements of exceeding the minimum threshold or not. If a given system does not meet the requirements set for it, it should be improved. The effectiveness of the systems can be increased by replacing the detection and neutralisation devices with better ones or by changing the operating conditions of these devices. For example, a change in conditions means the removal of bushes and trees from the vicinity of the protected object for radar detection. If the above-described actions do not bring improvement, anti-drone prevention methods should be applied.

The sequence of events in the drone attack is shown in the diagram.

UAVs are a source of danger to facilities and people. The activation of this threat consists in the fact that the pilot takes the control apparatus in his hand and takes off towards the target of the attack or programs the mission on the computer and indicates the protected object as the target of the attack. After the attack has started, defensive actions begin, which consist of detecting the drone and then neutralising the drone. After the attack is over, the consequences are assessed. As a consequence, losses or damage are generated in the human-technology-environment system.

Figure 3. Diagram presenting the sequence of events during a drone attack.



If the calculation of the probability of detection and neutralisation of the drone shows that the effectiveness of the system will be unacceptable, and other methods or replacing the devices with better ones or changing the operating conditions of these devices do not result in an improvement in effectiveness, following preventive measures should be considered:

- designation of drone geographic zones DRA-P (Drone Area – Prohibited) (Commission Implementing Regulation, 2019),
- undertaking activities for the benefit of the local community aimed at gaining its sympathy, which in turn may lead to greater control of the surroundings of the facility through more eyes,
- conducting training in the field of aviation law for police officers,
- conducting training in the field of pilotage for the personnel of the physical security of the facility, which in turn should familiarize the staff with the capabilities of unmanned aerial vehicles,
- masking elements of the protected facility in order to limit the amount of information obtained during an attack with the use of VIS and IR cameras,
- building covers of installation elements to prevent damage as a result of a direct impact with a drone or as a result of an explosion of explosives.

These activities have already been well described in the literature (Łukasiewicz *et al.*, 2021).

Conclusions

Unmanned aerial vehicles pose a threat to objects important to state security and to people. Currently built systems are ineffective and do not cope as desired with single aircraft. The situation will worsen when drone swarm technology becomes popular. An additional problem is the fact that most of the facilities important to the security of the state, including those currently classified as critical infrastructure facilities, Polish or European, were designed and built at a time when drones did exist, but were not so widely available in trade. and as widely used in everyday life as it is today. These objects are therefore vulnerable to a drone attack, and the probability of success of such an attack is high.

Due to the low effectiveness of anti-drone systems, efforts are being made to find new, more effective methods of detecting and neutralising drones. Due to the risk of an attack by a single drone, but also by a swarm of drones, both of these attack methods must be taken into account when assessing the effectiveness of drone detection and neutralisation systems. Of course, one can judge the effectiveness of detection and neutralisation experimentally, and this will give an overall picture of the effectiveness of the system. Nevertheless, only an experimentally confirmed mathematical model can give a precise picture.

To sum up:

- The paper proposes a mathematical model for assessing the effectiveness of detection system and the effectiveness of the neutralisation system, which are parts of the anti-drone system,

- The proposed model allows, on the basis of experimentally obtained data, the effectiveness of drone detection and neutralisation systems to be evaluated. Therefore, it enables the evaluation of the system in a comprehensive manner, and the mathematical description allows for the identification of inefficient elements of the detection and neutralisation system and thus the improvement of the effectiveness of the system as a whole,

- The proposed model is very simple, thanks to which an average educated member of the physical security personnel of the facility could independently assess the effectiveness of the anti-drone system, based on data such as the probability of detection and the probability of neutralisation of the drone under given conditions,

- Having access to the specific data of a given type of aircraft, such as an unmanned aircraft, an unmanned multirotor or an unmanned helicopter, including data on how to carry out an air mission and design data of the protected object obtained using Building Information Modelling methods, by using the system assessment model proposed in the paper, someone can simulate the effectiveness of the drone detection and neutralisation system using a computer program. A computer simulator of drone detection and neutralisation systems makes it possible to design a three-dimensional anti-drone system in the most efficient way for a given critical infrastructure facility and thus reduce the costs of investment in anti-drone systems by eliminating the purchase of inefficient devices that do not meet the expectations of the facility's physical security personnel at the initial design stage.

Funding

This research received no external funding.

Author Contributions

Conceptualization, J.Ł.; Methodology, J.Ł., Investigation, J.Ł. and A.K.T., Resources, J.Ł and A.K.T.; All authors read and agreed to the published version of the manuscript.

Data Availability Statement

Not applicable.

Disclosure statement

No potential conflict of interest was reported by the authors.

References

Abdalla, A.S., Powell, K., Marojevic, V. and Geraci, G. (2020) 'UAV-assisted attack prevention, detection, and recovery of 5G networks', *IEEE Wireless Communications*, 27(4), pp. 40–47. doi: 10.1109/MWC.01.1900545.

Abdullah, R.S.A., Saleh, N.L., Rahman, S.M.S.A., Zamri, N.S. and Rashid, N.E.A. (2019) 'Texture classification using spectral entropy of acoustic signal generated by a human echolocator', *Entropy*, 21, p. 963. doi: 10.3390/e21100963.

Aljazeera (2022) *Timeline: UAE under drone, missile attacks*. Available at: https://www.aljazeera.com/news/2022/2/3/timeline-uae-drone-missile-attacks-houthis-yemen (Accessed: 1 February 2022).

Al-Sa'd, M.F., Al-Ali, A., Mohamed, A., Khattab, T. and Erbad, A. (2019) 'RF-based drone detection and identification using deep learning approaches: An initiative towards a large open-source drone database', *Future Generation Computer Systems*, 100, pp. 86–97. doi: 10.1016/j.future.2019.05.007.

Andraši, P., Radišić, T., Muštra, M. and Ivošević J. (2017) 'Night-time detection of UAVs using thermal infrared camera', *Transportation Research Procedia*, 28, pp. 183–190. doi: 10.1016/j.trpro.2017.12.184.

Barisic, A., Car, M. and Bogdan, S. (2019) 'Vision-based system for a real-time detection and following of UAV', *Workshop on Research, Education and Development of Unmanned Aerial Systems (RED UAS)*, 2019, pp. 156–159. doi: 10.1109/REDUAS47371.2019.8999675.

BBC News (2018) *Venezuela President Maduro survives 'drone assassination attempt*. Available at: https://www.bbc.com/news/world-latin-america-45073385 (Accessed: 1 February 2022).

BBC News (2019) *Saudi oil attacks: Drones and missiles launched from Iran – US*. Available at: https://www.bbc.com/news/world-middle-east-49733558 (Accessed: 1 February 2022).

BBC News (2021) *Iraqi PM al-Kadhimi survives drone attack on his home*. Available at: https://www.bbc.com/news/world-middle-east-59195399 (Accessed: 1 February 2022).

BBC News (2022) *Sweden drones: Sightings reported over nuclear plants and palace*. Available at: https://www.bbc.com/news/world-europe-60035446 (Accessed: 1 February 2022).

Beamforming algorithms – beamformers, Jørgen Grythe, Norsonic AS, Oslo, Norway. Available at: https://web2.norsonic.com/wp-content/uploads/2016/10/TN-beamformers.pdf (Accessed: 1 February 2022).

Burshtein, D. and Weinstein, E. (2001) 'Signal enhancement using beamforming and nonstationarity with applications to speech', *IEEE Trans. Signal Processing*, 49, pp. 1614–1626. doi: 10.1109/78.934132.

Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems. Available at: https://eurlex.europa.eu/legalcontent/EN/TXT/?uri=CELEX:32019R09 45 (Accessed: 1 February 2022).

Consolidated text: Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft (Text with EEA relevance). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02019R0947-20210805 (Accessed: 1 February 2022).

Crino, S. and Dreby, C. "ANDY." (2020) *Drone attacks against critical infrastructure: A real and present threat*, Atlantic Council, 14 p. Available at: https://www.atlanticcouncil.org/wp-content/uploads/2020/05/DRONE-ATTACK-0420-WEB.pdf (Accessed: 1 February 2022).

DJI. (2002a) Available at: https://www.dji.com/pl/aeroscope (Accessed: 25 March 2022).

DJI. (2002b) Available at: https://www.dji.com/pl/products/compare-consumer-drones (Accessed: 25 March 2022).

European Commission (2017) 'Guidance on sampling methods for audit authorities. Programming periods 2007–2013 and 2014–2020', EGESIF_16-0014-01 20/01//2017. Available at: https://ec.europa.eu/regional_policy/sources/docgener/informat/2014/guidance_sampling_method_en.pdf (Accessed: 1 February 2022).

Ezuma, M., Anjinappa, C., Semkin, V. and Guvenc, I. (2021) 'Comparative analysis of radar cross section based UAV classification techniques'. pp. 1–16. doi: 10.13140/RG.2.2.12121.65125.

Ferreira, R., Gaspar, J., Sebastião, P. and Souto, N. (2022) 'A software defined radio based anti-UAV mobile system with Ja'ming and spoofing capabilities', *Sensors*, 22, p. 1487. doi: 10.3390/s22041487.

Gannot, S., Burshtein, D. and Weinstein, E. (2001) 'Signal enhancement using beamforming and nonstationarity with applications to speech', *IEEE Trans. Signal Processing*, 49, pp. 1614–1626. doi: 10.1109/78.934132.

Grisaro, H.Y., Turygan, S. and Sielicki, P.W. (2021) 'Concrete Slab Damage and Hazard from Close-In Detonation of Weaponized Commercial Unmanned Aerial Vehicles', *Journal of Structural Engineering*, 147(11). p. 04021190 doi: 10.1061/(ASCE)ST.1943-541X.0003158.

Guinness World (2021) Available at: https://www.guinnessworldrecords.com/news/commercial/2021/5/3281-drones-break-dazzling-record-for-most-airborne-simultaneously-655062 (Accessed: 29 March 2022).

Hambling, D. (2021) 'Drone used in attack on US electrical grid last year, report reveals', *New Scientist*. Available at: https://www.newscientist.com/article/2296480-drone-used-in-attack-on-us-electrical-grid-last-year-report-reveals/#ixzz7KPX5qdiT (Accessed: 1 February 2022).

He, F., Zhou, T., Xiong, W., Hasheminnasab, S.M. and Habib, A. (2018) 'Automated aerial triangulation for UAV-based mapping', *Remote Sens.*, 10, p. 1952. doi: 10.3390/rs10121952.

Hirabayashi, M., Kurosawa, K., Yokota, R., Imoto, D., Hawai, Y., Akiba, N., Tsuchiya, K., Kakuda, H., Tanabe, K. and Honma, M. (2020) 'Flying object detection system using an omnidirectional camera', *Forensic Science International: Digital Investigation*, 35, 301027. doi: 10.1016/j.fsidi.2020.301027.

Kasteloo, H. (2020) 'Drone DJ'. Available at: https://dronedj.com/2020/01/24/weaponized-dji-matrice-200-taliban-afghan-security-forces/ (Accessed: 1 February 2022).

Kapoor, R., Ramasamy, S., Gardi, A. and Sabatini, R. (2017) 'UAV navigation using signals of opportunity in urban environments', *A Review, Energy Procedia*, 110, pp. 377–383, ISSN 1876-6102. doi: 10.1016/j.egypro.2017.03.156.

Krauss, J.D. (1992) *Electromagnetics*, 4th ed., McGraw-Hill, New York, NY, ISBN 0-07-035621-1.

Łukasiewicz, J., Piekarski, M. and Kluczyński, M. (2021) 'Polish association for national security of critical infrastructure against threats from unmaned platforms', ISSN 2720-037X, Vol. II, 33 Available at: https://drive.google.com/file/d/1hCHNae2847TwpHQjE-KcBwAI4SreDt4Y/view (Accessed: 1 February 2022).

Maestre, N. del Rey, Mata-Moya, D., Jarabo-Amores, M., Gomez-del-Hoyo P. and Rosado-Sanz, J. (2019) 'Optimum beamforming to improve UAV's detection using DVB-T passive radars', in *2019 IEEE International Radar Conference (RADAR)*, 23–27 September 2019, Toulon, France, pp. 1–6. doi: 10.1109/RADAR41533.2019.171288.

Monnik, M. (2021) *A confronting look at Jihadi weaponisation of commercial drones*. Available at: https://dronesec.com/blog/a-confronting-look-at-jihadiweaponisation-of-commercial-drones (Accessed: 1 February 2022).

Ochodnický, J., Matousek, Z., Babjak, M. and Kurty, J. (2017) 'Drone detection by Ku-band battlefield radar', in *2017 International Conference on Military Technologies (ICMT)*, 23–27 September 2019, Toulon, France, pp. 613–616. doi: 10.1109/MILTECHS.2017.7988830.

Oh, J., Lim, D.W. and Kang, K.M. (2020) 'Unmanned aerial vehicle identification success probability with LoRa communication approach', in *2020 IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications*, 23–27 September 2019, Toulon, France, pp. 1–6. doi: 10.1109/PIMRC48278.2020.9217172.

Park, S., Kim, H.T., Lee, S., Joo, H. and Kim, H. (2021) 'Survey on anti-drone systems: Components, designs, and challenges', *IEEE Access, 9,* 42635–42659. [9378538]. doi: 10.1109/ACCESS.2021.3065926.

Pradier, P. (2018) 'Greenpeace intentionally crashes drone into French nuclear power plant to reveal security vulnerability', *Abcnews*. Available at: https://abcnews.go.com/International/greenpeace-intentionally-crashes-drone-french-nuclear-power-plant/story?id=56343027 (Accessed: 1 February 2022).

Quevedo, Á.D., Urzaiz, F.I., Menoyo, J.G. and López, A.A. (2018) 'Drone detection with X-band ubiquitous radar', in *2018 19th International Radar Symposium (IRS)*, 23–27 September 2019, Toulon, France, pp. 1–10. doi: 10.23919/IRS.2018.8447942.

Radartutorial. Available at: https://www.radartutorial.eu/06.antennas/Digital%20Beamforming.en.html (Accessed: 1 February 2022).

Sahmoudi, M. and Amin, M.G. (2009) 'Robust tracking of weak GPS signals in multipath and jamming environments', *Signal Processing*, 89(7), pp. 1320–1333, ISSN 0165-1684. doi: 10.1016/j.sigpro.2009.01.001.

Schäffer, B., Pieren, R., Heutschi, K., Wunderli, J.M. and Becker, S. (2021) 'Drone noise emission characteristics and noise effects on humans – A systematic review'. *International Journal of Environmental Research and Public Health*, 18(11), p. 5940. doi: 10.3390/ijerph18115940.

Singhal, G., Bansod, B. and Mathew, L. (2018) 'Unmanned aerial vehicle classification, applications and challenges: A review', Preprints, 2018110601. doi: 10.20944/preprints201811.0601.v1.

Solidakis, G.N. (2017) 'An Arduino-based subsystem for controlling UAVs through GSM', in *2017 6th International Conference on Modern Circuits and Systems Technologies (MOCAST)*, 23–27 September 2019, Toulon, France, pp. 1–4. doi: 10.1109/MOCAST.2017.7937656.

Swedish police hunt for drone seen flying over Forsmark nuclear plant. (2022) Reuters. Available at: https://www.reuters.com/world/europe/swedish-police-hunt-drone-seen-flying-over-forsmark-nuclear-plant-2022-01-15 (Accessed: 1 February 2022).

Tahir, A., Böling, J., Haghbayan, M.H., Toivonen, H.T. and Plosila, J. (2019) 'Swarms of unmanned aerial vehicles – A survey', *Journal of Industrial Information Integration*, 16, 100106, ISSN 2452-414X. doi: 10.1016/j.jii. 2019.100106.

The National Interest (2021) *Chinese engineers shot down a large drone using an electromagnetic pulse*. Available at: https://nationalinterest.org/blog/buzz/chinese-engineers-shot-down-large-drone-using-electromagnetic-pulse-192571 (Accessed: 1 February 2022).

Wu, Y., Sui, Y. and Wang, G. (2017) 'Vision-based real-time aerial object localization and tracking for UAV sensing system', *IEEE Access*, 5, pp. 23969–23978. doi: 10.1109/ACCESS.2017.2764419.

Yaacoub, J.-P., Noura, H., Salman, O. and Chehab, A. (2020) 'Security analysis of drone's systems: Attacks, limitations, and recommendations', *Internet of Things*, 11, 100218. doi: 10.1016/j.iot.2020.100218.

Zhou, C., Yan, Q., Shi, Y. and Sun, L. (2021) 'DoubleStar: Long-range attack towards depth estimation based obstacle avoidance in autonomous systems' , arXiv preprint. doi: 10.48550/arXiv.2110.03154.

Ziyang, Z., Dongjing, X. and Chen, G. (2018) 'Cooperative search-attack mission planning for multi-UAV based on intelligent self-organized algorithm', *Aerospace Science and Technology*, 76, pp. 402–411. doi: 10.1016/j.ast.2018.01.035.