IX INTERNATIONAL SCIENTIFIC PROFESSIONAL CONFERENCE
SECURITY AND CRISIS MANAGEMENT – THEORY AND PRACTICE (SeCMan)
- IX INTERNATIONAL FORUM „SAFETY FOR THE FUTURE 2023" -
29th and 30th September 2023, Belgrade, Republic of Serbia

COUNTERING THE THREAT OF UNMANNED AERIAL SYSTEMS TO CRITICAL INFRASTRUCTURE

Goran Maksimovic[1]

[1] Security Research Center, Street Sinise Mijatovica 9, Banja Luka, Republic of Srpska, Bosnia and Herzegovina, gomax5575@yahoo.com

Received: 27th July 2023
Accepted: 22th August 2023

Original scientific paper

Abstract: *It has been observed that unmanned aerial systems (UASs), have been used in a very different way over time including both the malevolent and benevolent usage. Today, technologicaly developed society, demands regular provision of resources vital for own functioning whilst being heavy sensitive on its disruption. Unmanned aerial systems could pose a threat to facilities critical to the functioning of the population and the government. Having in mind their abilities, the ways they could be used malovolently is practically unlimited. Nowdays, ensuring the acceptable level of security for critical infrastructure includes the counter-UAS system as well. This paper proposes a method for building a security system for encountering the malevolent usage of UAS and allows effectiveness of the C-UAS to be assessed.*

Key words: *critical infrastructure, unmanned aerial system, detection and neutralization, C-UAS*

1. INTRODUCTION

Contemporary, technologicaly developed society, demands regular provision of resources vital for own functioning, not requesting unnecessary pilling of suppies concurrently being heavy sensitive on its disruption. The world today has seen a number of developments as result of technological advancments. These outcomes have been demonstrated to be more trustworthy, approachable and economical in everyday lives. In addition, people now engage with one another in other ways inside their social circles. On the other side, unmanned aerial systems (UASs) are employed for both commercial and private purposes in addition to being heavily utilized in military contexts. Consequently, unmanned aerial systems could pose a threat to facilities critical to the functioning of the population and the government.

The attempt of this article is to give a comprehensive understanding of new advancements that have led to the issues surrounding unmanned aerial systems (UASs), including mostly threats, privacy concerns and other limits that are important and cannot be disregarded. A working hypothesis is that current security measures are not developed enough to adress the threat posed by UAS and need to be developed further. The major goal is to identify most of the issues related to this and to give all scholars access to a single resource that will allow them to understand the most recent trends and a thorough understanding of the subject. This paper has been organized in to five sections. The first part of the paper deals with the term of critical

infrastructure, the second is focused on determination and UAS characteristics while the section three contains options of malicious usage of the UAS. Vulnerability of the UAS is in the fourth chapter and the last one is dealing with the modes of countering the UAS threat. The overall conclusion to this work can be found on the end.

2. CRITICAL INFRASTRUCTURE AND ITS PROTECTION

Today's society requires a regular supply of resources necessary for its functioning and does not require unnecessary stockpiling, which is at the same time sensitive to supply interruptions. Because of this, the priority of protection is focused on the infrastructure that makes it possible, marked as critical. Etymologically, the adjective "critical" gives special importance to the functioning of what that adjective describes. Therefore, the term Critical Infrastructure (CI) refers to those physical resources, services and capacities of information technology, networks and infrastructure that, if disrupted or destroyed, can have serious consequences for the health, safety or economic well-being of citizens or the effective functioning of the government. Factors that make them extremely vulnerable are present in CI: complexity, interdependence and cascading effect. One of the most frequently identified shortcomings related to the protection of critical infrastructure is an incomplete understanding of the interdependence of these infrastructures.

There are two approaches to defining the term critical infrastructure: traditional, which identifies specific facilities and objects of social interest, and holistic, which focuses on the complete system, networks and their interdependence. (Maksimovic, 2022,) Although there are different approaches to its determination, basically, critical infrastructure is made up of numerous sectors. Critical infrastructure is characterized by interconnectedness so that a break in the functioning of one element of the system can lead to a break in another, i.e. to a cascade effect, causing long-term consequences for the government system, economy, security, public health and public trust. It is the mutual connection that causes the threat of one element of the critical infrastructure system to lead to a multiply increased effect of the attack and the consequences on a number of other elements of the critical infrastructure, as well as on economic stability and society as a whole.

However, complete protection does not exist and the effects of malicious activity on critical infrastructure can be reduced by risk assessment and crisis planning. Taking measures to protect critical infrastructure requires constant dialogue between the technical and security community. Protecting CI is not a new phenomenon and it is perceived from different points of view: technical, defense, economic, national security, etc. The topicality of the protection of elements of CI stems from the fact that they are connected and highly vulnerable, the increase in the number of malicious activities aimed at citizens, as well as the increasing impact of climate change. Protection represents readiness, rejection, mitigation, response or recovery from disruption or destruction of CI. These activities are aimed on preserving the performance of CI in the event of the inability to provide a defined minimum level of service and minimizing damages and shortening recovery time. Only with a systematic analysis can the object of protection, the time of onset of protection measures, definition of tactics, techniques and procedures, etc. be determined. As the nature of hazards changes rapidly and continuously, corrective measures and responses also need to be adaptive. The protection of CI is approached traditionally - by identifying specific facilities and objects and developing plans for their protection, and by a modern scientific approach (holistic) - focused on the network system and their interdependence. The measures used to achieve safety and protection of CI include personnel, technical, structural and technological measures and physical security measures. Critical infrastructure risk analysis is necessary at all levels, horizontally and vertically, using the same methods and instruments and it precedes the creation of a vulnerability assessment.

The goal of the CI protection process is to ensure the desired level of physical protection and resistance of CI elements to the effects of all threats and the recovery process in case of element function degradation. The basic standards and rules for the CI protection are included in the context of the process of building the security framework in which the CI protection system will be built. It should determine criteria for the selection of CI facilities, emphasize the importance of CI and requirements for physical protection and should be based on the specification of CI elements. There are usually three to five classes of protection and the classification is based on the measure of the impact that disabling an element of CI. Degradation levels are defined without compromising basic function, with compromising basic function and complete incapacitation. The critical infrastructure protection system creates a critical infrastructure management system. Achieving infrastructure protection, resilience and recovery include security assessment of CI elements, security measures specifications and reconstruction functions. The organization of the critical infrastructure protection system contains a number of conceptual, organizational, technological and technical measures that ensure the required level of protection of CI elements.

3. UAS DETERMINATION AND CHARACTERISTICS

3.1. Terminology and typology

The term unmanned aerial system (UAS) applies to the unmanned aerial vehicle and its associated elements, including communication links and UAS control components, which are required for the operator to maneuver efficiently in the airspace. An unmanned aerial vehicle (UAV) is an aircraft operated without direct human intervention in or on the aircraft. As noted, UAS include three key components: aircraft (UAV), a ground control system (GCS) and a bi-directional link between the UAV and the GCS (Table 1) (Ghulam et.al., 2022; Siddiqi et.al, 2022). A UAV can be controlled autonomously without a pilot and can be controlled remotely. Today, one may see the variety of several UAS being opted for commercial and domestic use mainly because they are cost effective and are controlled remotely from anywhere.

Table 1. UAS Frequencies communication link *(Source: Author)*

Sr.No	Bandwidth	Description	Purpose
1.	2400.000–2483.500 MHz	≤ 100mW, if the associated standard is EN 300 328 (Digital wideband data transmission equipment) ≤ 10mW, if the appropriate standard is EN 300 440 (General short-range devices).	Mostly used for short-range surveillance or short-range maneuvering missions.
2.	5470.000–5725.000 MHz	The transmitter's operational power is ≤ 1W and the power spectral density of transmission is ≤ 50mW/1 MHz. The appropriate standard is EN 301 893 (RLAN equipment).	Long stay in sky operations, used mainly for aerial photography.
3.	5725.000–5875.000 MHz	The transmitter's operative power is ≤ 25mW and the appropriate standard is EN 300 440 (General short-range devices)	Used for short-range surveillance with fast maneuvering and manipulating tasks.
4.	5030–5091 MHz	As per the International Telecommunication Union ITU, the frequency is assigned to the command and control of UAV or drones in cargo and passenger traffic and so it cannot be used for ground-based UAVs or drones.	Used in such operations where data sharing is important with ground control room (GCR)

There are various types of UAV and discussing mainly the UAV, they could be classified into four main categories as follows: rotary-wing, fixed-wing, hybrid-wing and flapping-wing. The one with a vertical take-off and landing (VTOL) feature and that can hover at a high rate are known as rotary wing. The other with the horizontal take-off and landing (HTOL) and capability to fly aggressively and glide even with heavy payloads belong to fixed-wing. Lastly, the UAVs that have both fixed and rotary wings are known as hybrid-wing. They are designed

to have features of both previously mentioned. Some of them are designed to exhibit the flying motion of an insect and here they proposed a more power-efficient wing by changing the wing stiffener pattern parametrically (de Croon et.al, 2012). An aerodynamic analysis found that this could relate to increased wing stiffness as well as indications of vortex generation during the flap cycle. The experiments reported an improved generated lift, and scaling later these flapping-wings to flapping-wing microair vehicles (FWMAVs) having the ability to perform activities in urban and interior environments. However, the successful flight of these vehicles that are replicating insect flight, has many obstacles, including their design, manufacture, control, and propulsion.

It is already shown that any UAV can be controlled remotely using a ground command and control mechanism. Therefore, these UAVs are classified based on their ability to fly over long distances without any intervention as: fully autonomous, remotely operated and remotely pilot-controlled. The military purpose UAVs have some advanced sensors, not available on commercial base, enabling it to carry additional payloads. Subdivision of UAVs could also go into five major components as follows: airframe, onboard controller, payload capability, communication system and efficient batteries. When discussing the airframe, it must consider aerodynamics, a lightweight structure and stability but the payload variation as well. Another important component is the communication system which will ensure the communication and control between a UAV and GCS. Lastly, there is a reliable power source that can help it to fly for a specific time to fulfil the task.

Table 2. UAS communication technology (Ghulam et al.,2022)

Technique	Channel Width	Band	Bit Rate	Range	Latency	Mobility Support
Wi-Fi	20 MHz	2.4 GHz to 5.2 GHz	6–54 Mbps	100 m	10 ms	Low
GPS	2 MHz	1176 to 1576 MHz	50 bps	-	10 ms	Higher
UMTS	5 MHz	700 to 2600 MHz	2 Mbps	10 Km	20–70 ms	High
5G	2.16 GHz	57 to 64 GHz	Up to 4 Gbps	50 m	-	Ultra-High
LTE	20 MHz	700 to 2690 MHz	Up to 300 Mbps	30 Km	10 ms	Very High
LTE-A	Up to 100 MHz	450 MHz to 4.99 GHz	Up to 1 Gbps		-	Very High

Type of Communication	Elevation in Km	Number of Satellites	Satellite Life	Handoff Frequency	Doppler	Gateway Cost	Propagation Path Loss
Geostationary Earth orbit (GEO)	Up to 36,000	3, no polar coverage	15+	NA	Low	Very expensive	Highest
Medium Earth orbit (MEO)	5000–15,000	8–20 global	10–15	Low	Medium	Expensive	High
Low Earth orbit (LEO)	500–1500	40–800 global	3–7	High	High	Cheap	Least

It could be seen in Table 2, the UAS communicates the different wireless communication methods, but at the same time, it shares that the communication will have a latency rate as well. The table also shares the channel width, band interval and most importantly, the mobility support important for UAV design. The table represents a type of communication based on satellite type of each satellite communication.

3.2. Security vulnerabilities and concerns for UAS

For UAS there is neither a standardization of policies nor the availability of wireless security which leads to several threats. Such practical validations include the crashing of UAS with many parallel requests whereas some researchers pointed out on different types of UAS vulnerability. (Siddiqi et al., 2022) Generalyy, most attacks are softver based, targeting the operating system or the microcontroller of the UAV. Since there are huge advancements in the technology, UAS have a high probability of experiencing such attacks, such as GPS spoofing,

signal jamming or de-authentication. The most common vulnerability types to the UAV encompass the following: malware issue, spoofing, manipulation and other common concerns, physical design and control system limitation, sensors, Wi- Fi constraints, GPS issue, firmware issue, Skyjack attacks and controller issue. (Siddiqi et al., 2022) UAS offer numerous increasing benefits with technological progress although, some of them have limited operating resources and others create diverse security, privacy and safety issues. Licensing, regularization, and over-sight and surveillance-regulating measures and regulations are a priority. As regards, network security point at the risk analysis, it is an admitted fact that the coverage is quite different as compared to any sort of wireless sensor network or any mobile ad hoc networks. The reason lays behind the resource constraints, as UAV related coverage is broader and wider than afore mantioned.

The framework that sets the rules to operate UAS in any vicinity is known as authentication, authorization and accounting (AAA), which states several privileges to the UAS controller to operate as per the mentioned administrative rights. Moreover, in case of any uncertainty or illegal activity by UAS, it is possible easily track down the operator. This is done to limit illegal surveillance, cyberattacks and privacy threats. Thus, several mechatronic engineering solutions have been presented to overcome these malicious activities. Concerning AAA, the following guidelines could be effective for UASs:

- Authorization: assigning privileges to the UAS controller to avoid any hostile takeover with administrative rights,

- Authentication: need for a rigid authentication method for UASs to avoid unauthorized access and control,

- Accounting: in case of any illegal activity by a UAS, the owner can be tracked.

Various mechanical and operational capabilities of UAS are being exploited for conducting malicious activities. Such events make UAS growth a double-edgeds word, the effort to make them more secure and rigid also makes them more effective for malicious activities.

Due to their portability, low cost, availability, maintenability and maneuverability UAS are a perfect choice for malicious activity. The ability to carry a wide range of attachments makes them an effective couriers for harmful items. They can carry anything, unnoticed or stealthily. Security is not the only concern for UASs. Any UAS flying over populated areas or property can malfunction and crash and that could be harmful to buildings and can injure people. It is a high probability that a UAS can be hacked or may deviate from its path due to heavy weather disturbance. Thus, there should be a reset option available which may turn the UAS to a hovering condition only and help to gain the control back. There are certain areas where UAS may face signal jammers and later, can be controlled for a cyberattack. Thus, UAS could have some sort of filter that may detect if there is any signal jammer nearby.The third safety measure is related to its design, it is necessary to avoid any harmduring a crash.

3.3. Potential malicious application of UAS

UASs could be utilized generaly in both purposes, malicious and beneficient. The malicious usage represents the areas and specific domains where we are witnessing an incremental increase in utilizing the UAS over the last few decades. Factors such as diligence, cost, mobility in the humans unreachable areas, payload options and risk, compel everyone to use it. Now, depending on the type of UAS, they may be used in a efficient way. Commonly, it is seen that the UAS design is dependent on the type of mission they perform in the field. Thus, categorizing them all with respect to their domains may lead to understanding their architecture in a better way.

An UAS is a universal platform that can endanger a target from different heights, with different speeds, on different flight trajectories and with different on-board equipment. It could be used to damage an object by physically hitting or transporting a device or element that will damage the target. It could be perceived as a threat, based on the totality of circumstances that their activity may encompass: cause physical harm to a person, damage property, assets, facilities or systems, interfere with the mission of a covered facility or asset, including its movement, security or protection, facilitate or constitute unlawful activity, interfere with the preparation or execution of an authorized government activity, including the authorized movement of persons, result in unauthorized surveillance or reconnaissance or result in unauthorized access to or disclosure of classified, sensitive, or otherwise lawfully protected information and many others. Many UAS incidents are caused by careless or reckless operators but an adversary can also use it in a variety of malicious ways, including mainly the following:

- Active - taken through physical, material means physicaly endangering the object of attack,

- Passive - logical, elektromagnetic, cyber or behavioral means of endangering the object of attack.

A facility risk assesment should consider the totality of threats posed by UAS, whether these threats are caused by negligent or reckless use of UAS, criminality, terrorism or espionage. The risks associated with UAS should not be considered in isolation of other prevailing threat conditions. Considering the full range of threats will facilitate the development of a risk-based mitigation strategy that minimizes risks most pertinent to the specific object of prootection. When considering the likelihood of adversary UAS usage, it is important to consider the intent, the capability of the adversary and the desired effect. The potential of UAS has been proved already and this domain covers every type of utilization in PMESII (PMESII – political, military, economic, social, intelligence and information) purpose. Equipping the UASs with apropriate equipment multiplies its applications and increases efficiency.

Thoday, the UAS are low cost and easily available in markets and therefore, they are easy to use for any sort of malicious activity. Their ability to carry a wide range of external payloads make them more dangerous. Moreover, their ability to reach places where human beings cannot, makes them even more lethal because they can deliver anything without coming under anyone's notice.

4. COUNTERING THE THREAT OF UNMANNED SYSTEMS

When considering the issue of countering the UAS as a threat to CI, it is mainly focused on three areas: deterence, detection and neutralisation. Deterence encompass a set of measures of limitation of access, education of security personel, imposing the risk of legal sanctions when malicious use in question or conducting a form of information/media actions in order to deter possible attempt of attack. This measures encompass, having in mind issues mentioned in chapter 3.2., but are not limited to the following: UAS licencing, tracking the import of UAS, firmer law restrictions on use of UAS, especialy in field of CI, designation of UAS geographic restricted/prohibited zones (UASA-R/P), increasing local community activities for building a greater cooperation which lead to greater control of the surroundings of the facility, conducting training in the field of aviation law for police, conducting training in the field of pilotage for the personnel of the physical security of the facility, masking elements of the protected facility in order to limit the amount of information obtained during an attack, building covers of installation elements to prevent damage as a result of a direct impact with a UAS or as a result of an explosion of explosives.

The current detection **s**ystems, as elements of counter-UAS (C-UAS) systems that protect facilities, operate using various features of UAV: heat, noise, the shape of the aircraft and

electromagnetic radiation of various frequencies. (Yaacoub et al., 2020; Andrasi et al., 2017). Detection of heat is achieved by cameras operating in the infrared band of electromagnetic radiation The source of heat could be a lithium-polymer battery which is a usuall 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 but it is possible to design the UAS in such a way that the heat emitted by it is dissipated. Methods for dissipating heat in airplanes are alreready known. In the case of UAS, 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. However, detecting an aircraft with a microphone is relatively difficult especially because UAS may be constructed so that the propeller rotation speed is low. The rotation speed can be reduced by using larger diameter propellers resulting, little noise is emitted by the propeller. Another method may be to perform a gliding flight. Additionally, the 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. The detection efficiency of acoustic signal could be improved by using microphone arrays (Burshtein and Weinstein, 2001) but note that intensity of sound is inversely proportional to the square of the distance. The aircraft can be detected using visual methods but weather conditions are a prerequisite for detection, particularly night, fog and precipitation that could reduce the effectiveness of vision detection. There is a potential of artificial intelligence technology, that can identify the UAS on the basis of learned algorithms. The disadvantage of this system is the difficulty in teaching the system to recognise an object correctly because such approach is a long and difficult process. Additionally, if the intruder knows the rules of detection, he can build a UAS with an unusual shape. Detection is possible by detecting communication between a UAV and GCS but this is also an unreliable, inefficient method, particularly because the ability to perform an flight without communication with the GCS. Communication could also be protected by frequency hopping. Detection is possible with the radar as well, 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 (Maestre et al., 2019) but its effectiveness depends on distance between the UAV and the antenna.

The existing methods for neutralising UAS are not fully effective and therefore, neutralisation systems consist of devices whose operation is based on different principles. One of the neutralising methods is destroying it with laser light. The high-energy light beam may cause the UAS to fall after being hit. These systems requires good weather conditions due to the laser light is scattered on the bad water. An UAS neutralised by this method is in an uncontrolled manner because the fall could have serious consequences. This includes possible injuries of the people, fall on sensitive elements of the installations of the protected facility and inability to read the data stored on its computer. Another method of neutralisation is to catch a drone in a net. 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 UAS as element of the facility security system. This method is effective at close range and data can be read. Another way to neutralise a UAS is an electromagnetic pulse. The range of this type of impulse can be several kilometres and is aplicable on a typical UAS. Use of the UAS field by Faraday shield (Krauss, 1992) and filters placed on the electric wires in the UAV's housing, present counter C-UAS measures. Communication signal jamming between an UAV and GCS could be disturbed by the emission of an electromagnetic wave with a flat spectrum and the noise intensity uniform for all emitted frequencies. A frequently used method for neutralising a UAV is to distort the signal of the satellite positioning system (jamming) or spoof the system

(spoofing) (Sahmoudi & Amin, 2009). The disturbance is that a signal is emitted from the interfering device at the frequencies at which the positioning system works using interfering signal that is more powerful than the satellite signal and the UAS is not able to correctly determine its position. Spoofing is where a spoofing device emits a signal containing a falsified position. The UAV 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 UAV to be determined in the absence of access to the signal of the positioning system. 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 UAV by cheating the algorithms of analysing the image recorded by the UAV's camera (Zhou et al., 2021). This method takes advantage of the weakness in which the image analysis algorithm miscalculates the UAS'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 UAS's flight.

Rule-based threat detection is a new approach enabled by artificial intelligence (AI). In comparison to others, it is more reliant on technology and less on manual interaction. Signature-based detection works well for recognizing known threats, using a pre-programmed list of known threats and their indicators of compromise to operate. This could be a distinctive behavior that typically precedes a malicious network attack. A signature-based intrusion detection systems (IDS) examines network packets and compares them to a database of known indicators or attack signatures to detect any suspicious behavior. Anomaly-based IDS, on the other hand, could alert unusual behavior. Rather than looking for known indicators, anomaly-based IDS simply detects any unusual behavior to generate alarms.

To identify the false data injection attacks, one may use the rule-based approach, used to target the signal strength between the UAV and GCR. Some research papers have proposed a signature-based IDS over UAV where they addressed bioinspired cyberattacks associated with airborn networks (Yagdereli et.al., 2015). Last, is the anomaly-based IDS scheme which is used against jamming attacks. The only limitation of anomaly IDS is the huge resource requirement. They are complex and difficult to identify but, both, perpetrator and method of attack, can be identified. With this, appropriate countermeasures can be implemented to avoid any future incident. In meantime, incidents among airplanes and UAS address UAS security and privacy issues. Due to an increase in cyberattacks on UASs, there is a need to introduce strict policies and standards to minimize it. With the popularity of UASs, malicious and the illegal use of UASs will likely to proliferate.

The UAS countermeasures are divided into physical and local countermeasures, which are already proposed but still can be improved. The first countermeasure for resolving security threats on UAS is classifying the attacks types, intended target and objective of the attack. There is a need to highlight the nature of the attack and some security measures against the attacks. Most of the attacks target the authentication process of a UAS which imposes need for improvement in the UAS authentication method. The wireless-based communication network suffers from numerous security issues and threats. In recent times, machine learning based intrusion detection systems have been quite successful against network threats.

The UAS detection and neutralisation systems are not sufficiently effective to detect and neutralise a UAV. Such systems should therefore be based on devices operating on different principles. The use of devices operating on different principles ensures that the system will fulfil its task in all conditions. Detection and neutralisation devices in physical protection systems are selected by assessing the probability of detecting and neutralising unwanted

activity in given conditions. Detection and neutralisation systems consisting of devices operating on different principles should also be built based on the effectiveness and probability of detecting and neutralising UAS in given conditions and in the required time. The detection and neutralisation probability assessment should take place in the same conditions as the drone detection devices are assessed. It can be performed by counting the number of detections and neutralisations of the UAV/100 flights. An additional parameter to be assessed must be the detection and neutralisation time, known as the required time. The required time is the time when a UAV is detected and neutralised early enough to activate any planned procedures in the event of an attack before to be unable to successfully end an attack. One such procedure could be to activate the neutralising devices and direct them towards the attacking UAV. The probability of UAV detection and neutralisation in given conditions and in the required time is marked as Pdn, with the „dn" index being the detection and neutralisation device (DND). The total probability of the UAS being detected and neutralised by a system made of N devices is given by the formula (Łukasiewic & Kobaszyńska – Twardowska, 2022):

$$Pdn = 1 - (1 - Pdn1)\,(1 - Pdn2)...(1 - PdnN) \quad (1)$$

When examining detection and neutralisation devices, security personnel should remember a few principles that determine the effectiveness (and thus the probability) of detection and neutralisation. As first, the DND 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 DND must not influence each other in any way. Secondly, the DN equipment and the entire system must be inspected periodically. It results from the fact that each technical object may be damaged, which will result in a radical decrease in the value of Pdn. The control is also due to the fact that every technical object is getting old. The DN system should also be tested whenever the system operating conditions change. Lastly, the priority for the protected facility manager should be to ensure effective DN of the attacking UAV and not the cost of building the system. When designing a protection system for the protected facility, the detection devices should be selected in a way that their operation does not adversely affect the operation of other devices used in the protected facility.

5. CONCLUSION

The use of UASs has increased dramatically, marking an era of autonomous systems and vehicles. Importance of UAS increases do to their benefits for both civil and military concerns. However, with this rise in usage, a severe security concerns are also evident. The most frequent reason why these sustems are chosen in any covert use is because they are accesible, available and inexpensive to obtain. There have been numerous scholar contributions that have already addressed the countermeasures, however, there are still some areas that have not been addressed and can, therefore, still be exploited for any negative purposes. In this current, technological age, these two challenges cannot be disregarded.

UAV pose a threat to facilities critical to the functioning of the population and the government. Currently built and available systems are ineffective and do not cope with the threat as desired. The situation will deteriorate when UAS swarm technology becomes popular. An additional problem is the fact that most of the facilities important to the functioning of the population, classified as critical infrastructure facilities, were designed and built at a time when UAS did not exist, and the UAS were not so widely available and used in everyday life. These objects are therefore vulnerable to a UAS attack with high probability of success. The risk of an attack by a single UAS, but also by a UAS swarm, highlights the neccecity of both of these attack methods to be taken into consideration when assessing the effectiveness of UAS DN systems. Due to the low effectiveness of C-UAS systems, and permanent building of counter counter

measures, huge efforts are being made to find new, more effective methods of UAS detecting and neutralising. So, when it comes to the begining, a working hypothesis that current security measures are not developed enough to adress the threat posed by UAS and that detection and neutralisation systems are not sufficiently effective is confirmed.

Nevertheless, only an experimentally confirmed mathematical model can give a precise picture. This paper proposes a mathematical model for assessing the effectiveness of DN system, which is parts of the C-UAS system. The proposed model allows, DN systems to be evaluated and identification of inefficient elements and thus the improvement of the effectiveness of the system as a whole, It is also possible to obtain a softver that will support this assesment, based on this proposed mathematical model of DN system. It also makes it possible to design a three-dimensional C-UAS system in the most efficient way for a given critical infrastructure facility and thus reduce the costs of investment in C-UAS 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.

As a minimum, this paper offers an examination of theese pressing issues by providing a summary of the causes, as well as potential solutions although this paper presents some existing solutions and a number of recommendations.

REFERENCES

Andrasi, P., Radisic, T., Mustra, Mario and Ivosevic J. (2017). Night-time detection of UAVs using thermal infrared camera, Transportation Research Procedia, 28.

Burshtein, D. and Weinstein, E. (2001). Signal enhancement using beamforming and nonstationarity with applications to speech, IEEE Trans. Signal Processing, 49.

de Croon, G., Groen, M., De Wagter, C., Remes, B., Ruijsink, R., van Oudheusden, B. (2012). Design, aerodynamics and autonomy of the DelFly. Bioinspir. Biomim.

Ghulam E. Mustafa A., Saiful Azrin B. M. Zulkifli, Rana Javed Masood ,Vijanth Sagayan Asirvadam and Anis, Laouti. (2022). Comprehensive Review of UAV Detection, Security,and Communication Advancements to Prevent Threats. Drones, Vol 6.

Krauss, J. (1992). Electromagnetics, 4th ed., McGraw-Hill, New York, NY.

Łukasiewic, J., 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.

Maestre, N., 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, IEEE International Radar Conference (RADAR), Toulon, France.

Максимовић, Г., (2022). Концепт приватно-јавног партнерства и заштита критичне инфраструктуре, Зборник Дискурс о критичној инфраструктури, ВПТШ, Добој.

Ochodnický, J., Matousek, Z., Babjak, M. and Kurty, J. (2017). Drone detection by Ku-band battlefield radar, International Conference on Military Technologies (ICMT), Toulon,

Quevedo, Á. D., Urzaiz, F. I., Menoyo, J. G. and López, A. A. (2018). Drone detection with X-band ubiquitous radar, International Radar Symposium (IRS), Toulon.

Sahmoudi, Mohamed and Amin, Moenes G. 2009. Robust tracking of weak GPS signals in multipath and jamming environments, Signal Processing, 89(7), pp. 1320–1333,

Siddiqi, M. A., Iwendi C., Kniezova J. and Noble A. (2022). Analysis on security-related concerns of unmanned aerial vehicle:attacks, limitations, and recommendations. Mathematical Biosciences and Engineering, Volume 19, Issue 3.

Yaacoub, J., Noura, H., Salman, O. and Chehabm, A. (2020). Security analysis of drone's systems: Attacks, limitations, and recommendations, Internet of Things.

Yagdereli, E., Gemci, Cemal and Aktas, A. Ziya. (2015). A Study on Cyber-Security of Autonomous and Unmanned Vehicles. The Journal of Defense Modeling and Simulation.

Zhang, G., Wu, Q., Cui, M., Zhang, R. (2019). Securing UAV Communications via Joint Trajectory and Power Control. IEEE Trans. Wirel. Commun. 18.

Zhou, C., Yan, Q., Shi, Y. and Sun, L. (2021). Double Star: Long-range attack towards depth estimation based obstacle avoidance in autonomous systems, arXiv preprint. https://arxiv.org/abs/2110.03154.