VII INTERNATIONAL SCIENTIFIC PROFESSIONAL CONFERENCE
SECURITY AND CRISIS MANAGEMENT – THEORY AND PRACTISE (SeCMan)
-SAFETY FOR THE FUTURE-

PROTECTION OF CRITICAL INFRASTRUCTURE FACILITIES AGAINST DROND ATTACKS USING DRONS

PhD Aleksandar Milić[1], MSc Marko Radovanović[2], PhD Aleksandar Petrovski[3]

[1] Military academy, University of Defence, Generala Pavla Jurisica Sturma 33, Belgrade, Republic of Serbia, milickm5@gmail.com

[2] 1st Army Brigade, Serbian Armed Forces, Dunavska 33, Novi Sad, Republic of Serbia, markoradovanovicgdb@yahoo.com

[3] University „Goce Delcev“, Military Academy „General Mihailo Apostolski“ Skopje, North Macedonia, aleksopetrovski@gmail.com

Abstract: *The issue of security and safety of infrastructures on which the functioning of modern society depends has become dominant and the issue of critical infrastructure is becoming crucial. Due to the complexity of the critical infrastructure system, which consists of a large number of elements of different types, its protection implies an interdisciplinary approach. Also, in the environment of increasingly global threats from terrorism and sabotage that can significantly affect the lives and health of the population, local economy and the environment, it is necessary to find fast and efficient solutions that will be applied both preventively and correctively.*

The development of weapons has conditioned the appearance of drones and anti-drone means for different purposes, which have a wide range of possibilities and are used in different spheres of society. The use of drones poses a great threat to the safety of critical infrastructure facilities, because there is a possibility of using both military and commercial drones for various illegal and terrorist purposes, thereby harming the economy and citizens.

Key words: *drone, UAV, security, critical infrastructure, weapon*

1. INTRODUCTION

The development of weapons and military equipment along with the development of terrorism and its expansion at the end of the XX and the beginning of the XXI century created the need to find effective models of protection. The most common targets of terrorist attacks were critical infrastructure facilities. Along with the development of terrorism, protection models and modern methods of combating terrorism have also developed. The security situation in the immediate vicinity and the support of terrorist organizations in the region indicate that there is a real possibility that Europe will be endangered by terrorist activities, directly or through the use of territory for the preparation and execution of terrorist activities in another country. The new effective weapon of terrorists is drones, which expanded in the second decade of the 21st century.

It is necessary to conduct a quality research on the possibility of protecting critical infrastructure facilities using drones from attacks by illegal drones. Drone attacks on critical infrastructure facilities represent a real threat to their safety. Research should be focused on analyzing the models of technical security of critical infrastructure facilities using different types and models of drones.

Today, modern society is facing the growing abuse of drones (drones) by terrorist and other controversial organizations motivated by different goals, but united in the same intention to seriously undermine the security of countries around the world. As a result, drones are becoming an increasing threat to the safety of people, critical infrastructure and other aircraft. They can be used for various illicit and dangerous purposes such as spying and intelligence gathering, smuggling or they can even be used as a weapon platform. Due to their size, low speed and low flight zone, it is very difficult to detect them and limit their movements from the aspect of protection of certain objects.

2. DEFINITION OF TERMS CRITICAL INFRASTRUCTURE AND DRONE

When it comes to critical infrastructure, there are several different definitions, but in general they all refer to assets and property, which are key to the smooth functioning of the economy and society. The United States considers critical infrastructure to be a basic resource whose term refers to the wide range of different assets and assets necessary for the day-to-day functioning of the social, economic, political, and cultural systems in the United States. Any disruption in critical infrastructure elements poses a serious threat to the proper, functioning of these systems and can lead to damage to property and human casualties and significant economic losses.

The analysis of the definitions of the term critical infrastructure concludes that the conceptual definition of the term critical infrastructure cannot be the same in all countries, and therefore the content must be determined at the national level. Defining the factors of critical infrastructure and their interdependence shows the importance of key resources of the state, the endangerment of which would disrupt the normal functioning of society. The definition of critical and key capacities by many organizations, institutions and analysts has become topical after recognizing the fact that they are far more vulnerable to terrorist challenges, risks and threats.[10] In Australia, critical infrastructure is physical facilities, supply chains, information technology and communication networks, which in the event of long-term neutralization or destruction would have a significant impact on the country's social and economic life, or affect the state's ability to maintain national defense and provide national security.

Critical infrastructure is the grouping of all resources that are essential for a country's telecommunications, energy, banking and finance, transportation, water and emergency services, both public and private. Critical infrastructure consists of physical, personal and cyber components.[5] To provide critical infrastructure means to provide a set of its factors from various dangers and threats, whether accidental or intentional. Effective protection of critical infrastructure facilities requires maintaining confidentiality at all levels.[15] Critical infrastructure protection requires the establishment of common software that will analyze every aspect, detailed analysis of the infrastructure, identification of hazards, risks and threats and that will warn of possible threats. The United States has defined 16 critical infrastructure sectors, namely: chemical sector, commercial facilities sector, communications sector, critical manufacturing sector, dam sector, defense industrial base sector, emergency services sector, energy sector, financial services sector, food and agriculture sector, government sector facilities, health case and public health sector, information technology sector, nuclear reactors, material and waste sector, transport system sector, water and wastewater system sector. [1,3]

Critical infrastructure must be secure and able to withstand and recover quickly from all threats and dangers, which requires proactive and coordinated efforts. Such efforts share responsibility between the various elements of the critical infrastructure system. Research needs to focus on investing and researching physical and cyber risk management tools and plans, educating a wide range of people about critical infrastructure security and resilience, business continuity plan, sharing threats and incident information, reporting and documenting

suspicious activities.[4] Drones with their wide range of possibilities in the future represent the main factor of the Critical Infrastructure Security System.

The term drone has a broad meaning, it is a means with a motor that is remotely controlled by the operator or it is a means that has a certain level of autonomy (control is achieved using communication software, and often artificial intelligence is used together with different types of sensors), which can be used once or more and can carry deadly or non-lethal cargo and transmit data in real-time.[6] It is a synthesis of the means and devices necessary to manage it. They differ in purpose, construction characteristics (shape, dimensions, weight, payload, maximum flight altitude, maximum range, flight time, speed, etc.), the environment in which they are used and the energy source that drives them. Depending on the purpose, they can be used in different environments such as land, water, air and space, and the broad spectrum of possibilities has enabled their use in defense and security (for the needs of the army and the police - original purpose) , agriculture, construction, traffic, trade, communication, science, medicine, research, architecture, video and photography, geology, forestry, mining, oceanography, environmental management, sports, mapping, etc. [9]

Žindrašič et al. in the paper *Modeling the organizational implementation of a drone and counter-drone operator into the Serbian Armed Forces rifle section* show different types of drones and anti-drone means.[14] Randjelović et al. in the paper *Anti - drone assets* [11] show the possibilities of using different types of anti - drone means, including drones. Samopjan et al. analyze different possibilities of using anti-drone means in the work *Analysis of anti-drone means*.[13] Detailed classification of drones was performed by Petrovski and Radovanović in the paper *Application of detection reconnaissance technologies used by drones in collaboration with C4IRS for military interested*. [9] The focus of the paper is on the presentation of air drones, ie UAVs with the possibilities of application in the protection of facilities and the possibilities and specifics of defense against attacks by other drones.

3. PROTECTION OF CRITICAL INFRASTRUCTURE FACILITIES

The most important difference in the use of artillery between NATO alliance and SA, can be defined as the fact that SA focuses on fire precision, and in NATO on fire speed, or timeliness of fire.

NATO artillery tactics are based on a “shoot and scoot” principle. This principle is developed with the assumption that the enemy always has both air and artillery supremacy. One battery can be given an assignment to carry out fire with a battery, platoon, pair or a single gun. The differences are well seen if we take on example the “Paladin” battery. This kind of unit, during operations, has the ability to fire upon multiple targets at the same time, even so every gun can acquire different fire [4]. The organization of security of critical infrastructure facilities includes planned and synchronized activities and application of measures, actions and procedures for the purpose of security protection of facilities. The goal is to completely neutralize and reduce the risk of potential security threats to the lowest possible level. Depending on the security assessment, the organization of security of critical infrastructure facilities also depends. Services and bodies that implement the protection of critical infrastructure facilities, are obliged to continuously monitor the sources, forms, activities, indicators aimed at endangering them and take measures to prevent adverse events.

Functional and quality security protection of important facilities must consist of multiple interrelated elements: normative-legal regulations in the field of security protection of critical infrastructure facilities (regulations and instructions), harmonization in planning and implementation of protection, through coordination of all elements in the security protection system, organizational structure of specialized services for providing and continuous

improvement of personnel and technical working conditions of specialized services.[7] Based on all the above, it is concluded that the security protection of critical infrastructure facilities is a complex task for specialized security services.

Security protection of facilities represents the scope of competencies, rights and duties of security entities of a state provided by legal regulations, which carry out measures, actions and procedures in order to ensure the highest level of protection of certain facilities, ie represents the entire activity that prevents and suppresses endangerment - threats to certain objects being protected.[7] Depending on the assessment of the security threat to a certain critical infrastructure facility, the model of securing it also depends. Based on the plan of security measures, the most efficient model of facility protection is applied. Security protection measures,[2] where each of the above measures, alone or in combination with one or more of them, represents a model for securing critical infrastructure facilities, are [12]: /1/ counterintelligence protection measures; /2/ preventive and security measures; /3/ preventive technical protection measures; /4/ physical - technical protection measures; /5/ preventive medical protection measures.

This part of the paper analyzes the application of technical protection measures with a focus on the possibilities of using drones in the provision and protection of critical infrastructure facilities. Technical protection measures represent a significant and indispensable segment of security protection of critical infrastructure facilities, which significantly contribute to raising the level of security of the facility, and without which it is not possible to organize effective security protection of critical infrastructure facilities. Technical protection measures include the use of modern technical means within the organized and planned activities of members of the facility security service, within which, depending on the characteristics of the facility, the use of technical protection means also depends. The most commonly used means for technical protection of the facility are: video surveillance cameras, motion sensors, thermal imaging cameras, alarm systems, pass registration and access control systems, protective lighting, means of communication, metal detectors, drones (using different types of sensors and cameras necessary for effective protection of buildings), etc. Drones have a wide range of applications in the protection of critical infrastructure due to the modularity of the use of different types of payload (cameras, sensors, software, radar, weapons).

4. PROTECTION OF CRITICAL INFRASTRUCTURE FACILITIES AGAINST DROND ATTACKS USING DRONS

In order to effectively protect critical infrastructure facilities from drone attacks from the air, a model of physical and technical protection using drones as an effective means of combating air drones was considered.

An anti-drone device is a type of device that neutralizes the action of a drone, where the drone: physically neutralizes or disables for further action, forces it to land at its position or at a predetermined location, takes control of drone commands, is forced to return to the starting position. The paper presents the possibilities of application of drones with the aim of presenting the possibilities of a wide range of applications of different types of drones in the fight against drones and in the protection of critical infrastructure facilities.

Drones are most often used in combination with other types of anti-drone means for the protection of critical infrastructure facilities and are used for detection, identification and neutralization. The use of drones in the protection of critical infrastructure facilities significantly increases the efficiency of their protection. Their use with adequate equipment allows:

- Timely detection of unwanted aircraft and warning of existing security risk and threat;

- Identification of illegal aircraft (photography, recording and tracking);
- Mobility in the protection zone of critical infrastructure facilities;
- Neutralization of illegal and unauthorized drones (drone hijacking, drone spoofing, geofencing, drone jamming, killer drones, drone capture and drone laser killer).

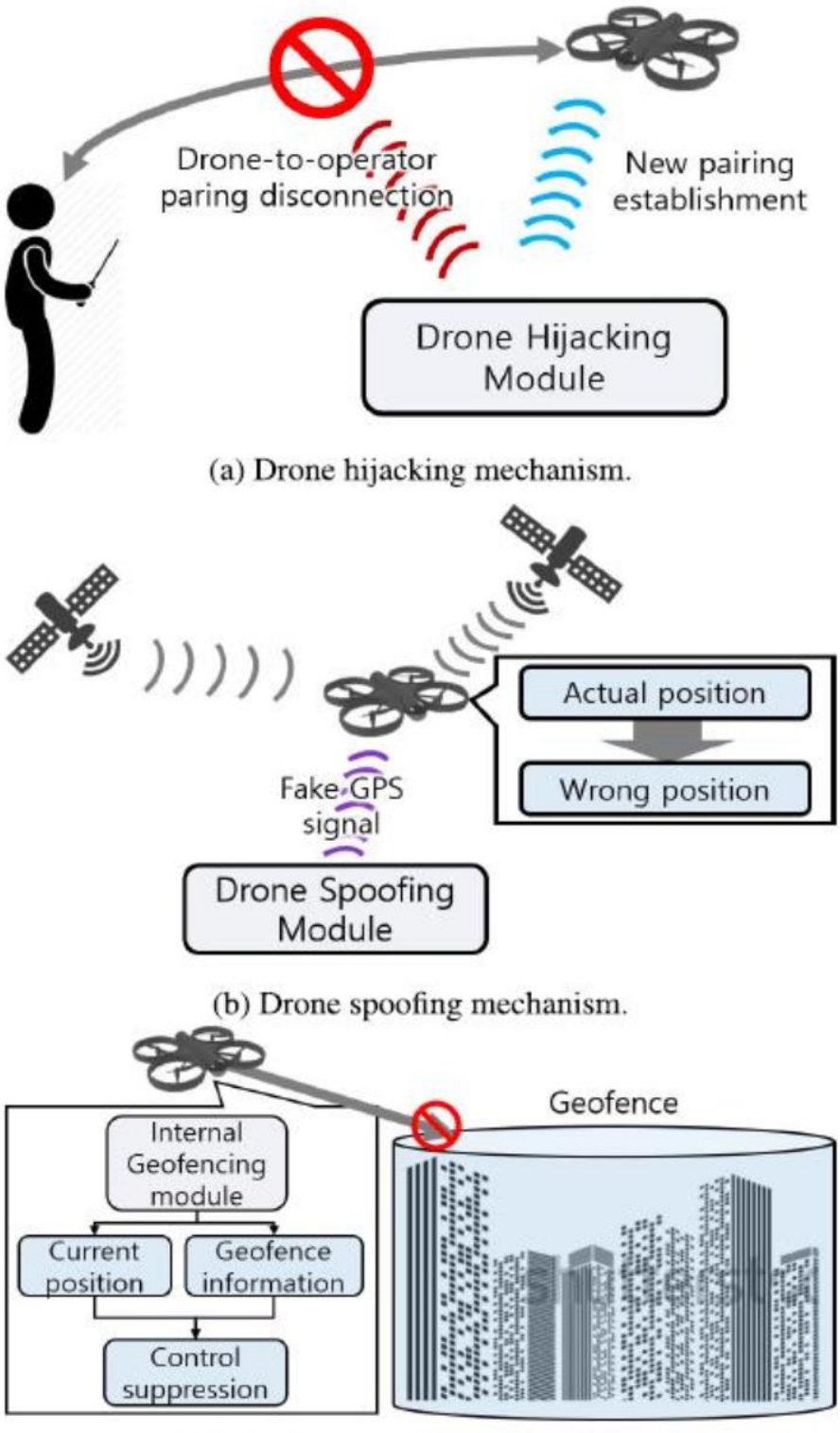

Figure 1. Typical non-destructive neutralization mechanisms [8]

To protect critical infrastructure facilities, it is possible to use a drone catcher, which neutralizes illegal drones by discharging the network and disabling further flight, an example of such a drone is shown in Figure 2. The use of such drones increases the degree of protection of critical infrastructure.

Figure 2. Drone catcher

One of the main problem of drones and UAV's is their autonomous, because more of them are performing tasks with minimal human intervention, using deep learning and variety of navigation and sensor data to determine where to fly. They are using geospatial data obtained in-flight but also used to train or assist with everything from flight paths to identifying objects in real time so UAV's and drones can make decisions on their flight. There are Five Levels to UAV's Autonomy /L 0/ fully manual control, /L1/ representing systems like altitude control but a pilot controls most of functions, /L2/ is multiple autonomous systems running together, but the pilot still has overall control, /L3/ means that the UAV can operate independently in some conditions, but the pilot can closely monitor the craft, /L4/ indicates the craft can fly and do practically all functions by itself but the pilot is a backup or can intervene occasionally and /L5/ is fully autonomy with no pilot involved. Current technology is between 3-4, with commercial, military and other UAV's using those levels. The main challenge of reaching L5 is a combination of technical challenges but also overcoming laws, regulations, and even social acceptance in different regions. Level 5 need sensors, radar and cameras to be able to function in any environment and all conditions, including inclement weather. We need to follow upgrading the drones and UAVs but in parallel we need to innovate contra measures how to protect our critical infrastructure by using of drones and UAV's. This will be a challenge of every society and every scientist who is a part of public security of critical infrastructure.

5. CONCLUSION

Creating effective models for the protection of critical infrastructure facilities is one of the main tasks of every state and is one of the most important factors influencing the national security of the state. The paper presents theoretical models of protection of critical infrastructure facilities from drone attacks using drones. Based on the analysis of the content of this model, it was concluded that the use of drones in the protection of critical infrastructure facilities significantly raises the level of safety and security of these facilities. This protection system is an effective model of protection of critical infrastructure facilities, but does not exclude the possibility of an attack on a protected facility.

Continuation of research should be directed towards the analysis of technical protection systems and selection of the most efficient system or combination of technical protection systems using drones and anti-drone systems, in order to find the most efficient model of critical infrastructure protection. By applying anti-drone systems in coordination with drones, it significantly increases the efficiency of protection of critical infrastructure facilities.

ACKNOWLEDGEMENTS

This paper was written under the VA-DH/1/21-23 project financed by the Ministry of Defense of the Republic of Serbia

REFERENCES

[1] Bayar M. (2019) Critical Infrastructure. In: Romaniuk S., Thapa M., Marton P. (eds) The Palgrave Encyclopedia of Global Security Studies. Palgrave Macmillan, Cham. Online ISBN: 978-3-319-74336-3

[2] Decree on determining the security protection of certain persons and facilities ("Official Gazette of RS", No. 72/2010).

[3] Di Pietro R., Raponi S., Caprolu M., Cresci S. (2021) Critical Infrastructure. In: New Dimensions of Information Warfare. Advances in Information Security, vol 84. Springer, Cham. pp. 157-196, eBook ISBN: 978-3-030-60618-3

[4] Georgescu A., Gheorghe A.V., Piso MI., Katina P.F. (2019) Critical Infrastructure. In: Critical Space Infrastructures. Topics in Safety, Risk, Reliability and Quality, Vol 36. Springer, Cham. pp. 1-19, Online ISBN: 978-3-030-12604-9

[5] Hentea, M. (2021). Critical Infrastructure. In Building an Effective Security Program for Distributed Energy Resources and Systems, M. Hentea (Ed.). pp. 211-241, Online ISBN: 9781119070740

[6] Milic, A., Ranđelovic, A., Radovanovic, M., (2019). Use of drones in operations in the urban environment, 5 th International Scientific conference Safety and crisis management – Theory and practise Safety for the future – SecMan, Belgrade, Serbia, (2019), pp. 124- 130, ISBN: 978-86-80692-04-3, Regional Association for Security and Crisis Management S4 GLOSEC Gobal security doo

[7] Nikolić, D., Kovač, M., Mitić V. (2018). Security protection of facilities of special importance for defense, Vojno delo, Vol. 70, no. 7, pp. 176 - 188, ISSN 0042-8426

[8] Park, S., Kim, H. T., Lee, S., Joo, H., Kim, H. (2021). Survey on Anti-Drone Systems: Components, Designs, and Challenges. in IEEE Access, Vol. 9, pp. 42635-42659, e-ISSN: 2169-3536

[9] Petrovski, A., Radovanović, M. (2021). Application of detection reconnaissance technologies use by drones in collaboration with C4IRS for military interested. Contemporary Macedonian Defense, Vol. 21, no. 40, pp. 117-126. e-ISSN 1857-887X

[10] Radovanović, M. (2018). The impact of terrorism on the protection of critical infrastructure of the defense industry of the Republic of Serbia. Proceedings of the First International Professional Conference in the Field of Critical Infrastructure Protection of the Defense Industry (ed. Beriša, H.), Belgrade.

[11] Randjelovic., A., Radovanovic, M., Stevanovic, M. (2020). Anti - drone assets. Proceedings of the 6th International Conference - Security and Crisis Management - Theory and Practice (eds. Komazec, N. and Babić, B.), pp. 35-41, Belgrade, October 2020, ISBN 978-86-80692-06-7, Regional Association for Security and Crisis Management-RASEC and S4 GLOSEC Global security

[12] Samopjan, M., Radovanovic, M. (2021). Models of securing residential facilities from terrorism. Proceedings of the 16th Conference with International Participation Risk and Safety Engineering (ed. Savić B.), pp. 195-202, Vrnjačka Banja, June 2021, ISBN 978-86-6211-126-5, Technical College of Vocational Studies in Novi Sad and Faculty of Technical Sciences - Department of Civil Engineering and Geodesy, Novi Sad.

[13] Samopjan, M., Radovanović, M., Stevanović, M., Polovina, U. (2020). Analysis of anti-drone means. Procedings of 11th DQM International conference Life Cycle Engineering and Management ICDQM - 2020 (ed. Ljubiša Papić), Prijevor,

[14] Žindrašič, V., Radovanović, M., Stevanović, D. (2020). Modeling the organizational implementation of a drone and counter-drone operator into the Serbian Armed Forces rifle section. Military work, Vol. 72, no. 3, pp. 84 - 109. ISSN: 0042-8426

[15] Zolesio, J.-L. (2013). Critical Infrastructure Protection. In Systems of Systems (eds D. Luzeaux and J.-R. Ruault). pp. 261-290, Online ISBN: 9781118557495).