IJAMEC
e-ISSN: 3023-4409

INTERNATIONAL JOURNAL OF APPLIED METHODS IN ELECTRONICS AND COMPUTERS

www.ijamec.org

International Open Access

Volume 11
Issue 04

December, 2023

*Research Article*

# Hybrid cyber security of unmanned aerial vehicles

***Orhun Dos[a, *], Yunus Emre Karakoca[b], Ebutalha Camadan[c], Fikret Baykali[d]***

[a]*Military Electronic Systems Engineering Department, Alparslan Defence Sciences and National Security Institute, National Defence University, Ankara, 06530, Türkiye*
[b]*Warfare Weapons and Tools Department, Alparslan Defence Sciences and National Security Institute, National Defence University, Ankara, 06530, Türkiye*
[c]*Computer Engineering Department, Army War College, National Defence University, Ankara, 06530, Türkiye*
[d]*Security Studies Department, Alparslan Defence Sciences and National Security Institute, National Defence University, Ankara, 06530, Türkiye*

ARTICLE INFO

*Article history:*
Received 12 June 2023
Accepted 27 November 2023

*Keywords:*
Cyber security
Unmanned aerial vehicle
Semi autonomous system
Military weapon systems
Hybrid security

ABSTRACT

Unmanned aerial vehicle technological improvement has had a direct influence on today's warfare. As today's battles take place in cities, the distinction between civilians and soldiers has grown increasingly hazy. There is a wealth of literature on autonomy and ethical concerns concerning autonomous weapon systems. Unmanned aerial vehicles must contend with a slew of security risks, ranging from electronic jammers to missile strikes. The societal acceptance of these techniques, ethical value judgments, and long-term consequences are all important topics to discuss. Unmanned aerial vehicles have a wide range of applications in the military, from gathering intelligence to destroying targets, and in the civilian arena, from agriculture to photography. Furthermore, unmanned aerial vehicles have the potential to be used not just for military or commercial goals, but also for international crimes. Nowadays unmanned aerial vehicles are used in electronic warfare to monitor enemy positions, prevent their communications by jamming systems, instantly monitor the country's border security, render the electronic systems of the determined targets inoperable, and listen for information via communication systems. Under the conditions specified above, the study seeks to provide a hybrid approach to unmanned aerial vehicles. The cybersecurity of unmanned aerial vehicles, software security, physical security, and social and cultural security will all be handled from a single point of view.

## 1. Introduction

Unmanned aerial vehicles (UAVs) have rapidly developed as a technology area in recent years, and their usage in various military, civil, and commercial areas is on the rise [1]. UAVs are vehicles that can perform tasks through remote control or autonomous systems and do not require human intervention [2]. These vehicles can collect data in real-time through high- resolution cameras, laser detection systems, and various sensors. They can be used in several areas such as air transport, reconnaissance and surveillance, agriculture, search and rescue, and can play a significant role on the battlefield [3]. However, the use of UAVs raises important ethical, legal, and safety issues that require a hybrid approach for examination.

This study will cover different security issues related to UAVs under a hybrid roof. Taking a hybrid approach to unmanned aerial vehicles, it is essential to have controlled aerial vehicles that can increase their journeys. The use of unmanned aerial vehicles is becoming increasingly common, not only for military purposes but also in the civilian field. Therefore, cyberattacks against aircraft or other security threats can pose significant risks.

In order to implement hybrid security measures, it is crucial to determine the necessary security measures for military aircraft. This includes physical security measures as well as software security and cyber security measures to prevent attacks against unmanned aerial vehicles. For example, devices used to monitor the flight of in-flight aircraft must be protected from cyberattacks or other security threats. In addition, the physical security of the services used in this center, such as aircraft and aircraft, is crucial. Social security is also essential for the acceptance of aircraft by society. Personal concerns regarding the use of drones cover not only safety but also ethical issues such as respect for privacy. Therefore, social acceptance for the use of aircraft is important for both civil and military

* Corresponding author. E-mail address: odos@kho.msu.edu.tr
DOI: 10.58190/ijamec.2023.65

purposes. Software and cyber security measures are among the most important steps to ensure the safety of unmanned aerial vehicles. These measures include using strong passwords, regularly updating software, and using firewalls and antivirus software. Physical security measures are crucial to ensuring the physical security of unmanned aerial vehicles. These measures include steps such as using locking devices, storing or protecting them in private areas, and using security cameras. Social acceptance is important for the widespread use of drones in society. Therefore, public concerns and respect for privacy regarding the use of drones should be taken into consideration. To achieve this, it is necessary to inform the public and make the use of unmanned aerial vehicles more acceptable in society. Table I shows the list of major abbreviations used throughout this study.

**Table 1.** List of major acronyms

| Notation | Meaning |
|---|---|
| UAV | Unmanned Aerial Vehicle |
| IDS | Intrusion Detection System |
| IPS | Intrusion Prevent System |
| ARP | Address Resolution Protocol |
| DNS | Domain Name System |
| RCC | Remote Control Command |
| EMI | Electromagnetic Interference |
| DOS | Denial of Service |
| DDOS | Distributed Denial of Service |
| VPN | Virtual Private Network |
| EW | Electronic Warfare |

This research aims to investigate various security concerns associated with safeguarding Unmanned Aerial Vehicles (UAVs) and to establish a foundation for their societal acceptance through a hybrid approach. In this context, an in-depth exploration of the cybersecurity, physical security, and social security aspects of UAVs have conducted.

## 2. Cyber Security of UAV's

Ensuring the cyber security of drones is a serious concern, and many measures need to be taken to prevent security breaches. In this part of the study, cyber security threats to unmanned aerial vehicles and the potential negative outcomes of these threats will be evaluated, and the cyber security measures that can be taken will be outlined. It is important to evaluate and classify the risks that may occur as a result of cyberattacks against unmanned aerial vehicles. The classification of cyber threats examined in our study is shown in Figure 1.

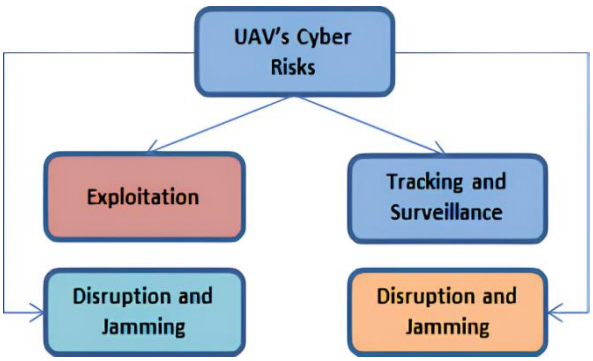


**Figure 1.** UAV's Cyber Risks Taxonomy

Exploitation: Unmanned aerial vehicles can be used as a tool by attackers to gain access to networks or data. In this case, attackers can damage systems, access data, or steal information using the UAV [4].

Tracking and Surveillance: Unmanned aerial vehicles can be used to track and spy on targets of attackers. By using the cameras of UAVs, attackers can track the positions, movements, and activities of targets [5].

Disruption and Jamming: Drones can be manipulated to cause attackers to take control of or interfere with the drone's missions. In this case, unmanned aerial vehicle operations will be disrupted or even completely stopped [6].

Occupation and Destruction: Drones can be manipulated in such a way that attackers can take control, causing them to use or destroy the drone for their own purposes. In this case, control of the unmanned aerial vehicle will be completely lost [7].

We believe that these threats pose a serious risk to the security of UAV systems. Therefore, when designing and implementing UAV systems, it is important to take the necessary measures to close security gaps. In 2011, Iran allegedly took control of a US drone (RQ-170 Sentinel) that it had captured [8]. This incident is an example of how vulnerable UAVs can be to cybersecurity vulnerabilities.

There are various types of cyberattacks against UAVs that can be carried out to take control of UAVs, steal data, or disrupt the missions of UAVs [9]. These cyberattacks can cause the risks mentioned in the previous section to occur. In addition, the consequences of cyberattacks against UAVs can be quite serious. For example, hijacking UAVs can give attackers access to sensitive information or allow them to make dangerous decisions regarding the use of the UAV [10]. Furthermore, taking control of UAVs may cause them to crash or inadvertently harm people. Therefore, it is important to classify the types of cyberattacks that may occur against unmanned aerial vehicles, as shown in Figure 2.

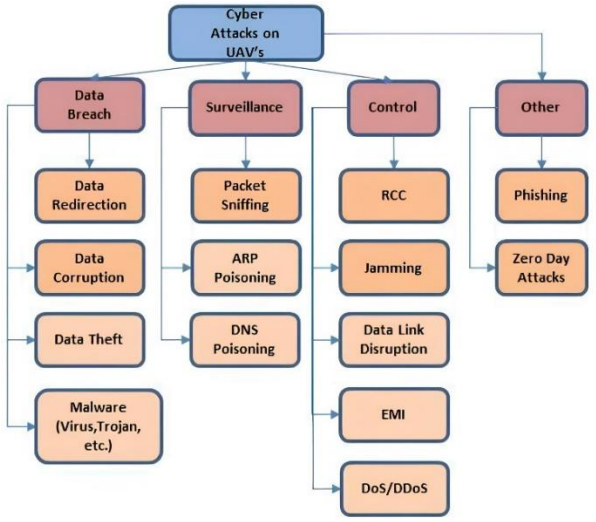


**Figure 2.** Types of Cyber Attacks on UAV's

The measures that can be taken for the cyber security of UAVs can be applied in many different areas, from the design of UAVs to data encryption. The cyber security measures that can be taken against the types of cyberattacks against UAVs are shown in Table II-V.

Data Redirection: Attackers try to take control of the UAV by interfering with the UAV's communication channels. In this way, they can direct the UAV as they wish.

Data Corruption: It refers to the corruption or alteration of data on UAVs.

Data Theft: For UAVs, it refers to the theft or capture of sensitive information.

Malware: Attackers make a malware attack on the UAV or the command and control system, causing hardware and software corruption or dysfunction.

**Table 2.** Cyber Security Measure For UAV (Data Breach)

| Types | Cyber Attack | Cyber Security Measure |
|---|---|---|
| Data Breach | Data Redirection | -Data Encryption,<br>-Authorization and Authentication,<br>-Secure Network Configuration |
| | Data Corruption | -Data Backup,<br>-Verification of Data Sources,<br>-Using Up-to-Date Software,<br>-Data Integrity Verification |
| | Data Theft | -Data Encryption,<br>-Strong Authentication,<br>-Using a Firewall<br>-System Updates |
| | Malware | -Using Safe Software Sources,<br>-Network Traffic Monitoring,<br>-Network Isolation(UAVs),<br>-Antivirus |

Packet Sniffing: Attackers monitor the communication channels of the UAV and capture the transmitted data. In this way, they can capture sensitive information.

ARP Poisoning: Attackers change the IP address of the UAV by interfering with the address resolution protocol in the UAV's communication channels. In this way, they can take over the communication channels of the UAV.

DNS Poisoning: It is accomplished by sending fake DNS responses by the attackers during the DNS resolution of the UAV. In this way, the communication channels of the UAV can be captured and the movements of the UAV can be monitored.

**Table 3.** Cyber Security Measure For UAV (Surveillance)

| Types | Cyber Attack | Cyber Security Measure |
|---|---|---|
| Surveillance | Packet Sniffing | -IDS,<br>-IPS,<br>-Encrypting Communication Channels |
| Surveillance | ARP Poisoning | -Updating ARP Tables,<br>-Secure Network Structure,<br>-Monitoring Network Traffic |
| | DNS Poisoning | -Update (DNS Servers) |

RCC: It aims to prevent the UAV from being controlled remotely. By intercepting or changing the control signals of the UAV, the attackers can change the route or movements of the UAV.

Jamming: It interrupts the control signals of the UAV by interfering with the control frequencies of the UAV. In this way, it may cause the UAV to become uncontrollable.

Data Link Disruption: It interrupts the data connection of the UAV by interfering with the communication channels of the UAV. In this way, it is not possible to control the UAV.

EMI: In this type of attack, attackers send electromagnetic interference to the electronic devices of the UAV. In this way, the electronic systems of the UAV may collapse and become uncontrollable.

Dos/DDoS: The operation of the system is hindered by sending a large amount of traffic to the systems in the UAV's communication network.

**Table 4.** Cyber Security Measure for UAV (Control)

| Types | Cyber Attack | Cyber Security Measure |
|---|---|---|
| Control | RCC | -Secure Connection (VPN) |
| | Jamming | -Frequency Diversity, Network Redundancy (Switching to other channels in case a channel is blocked), -Encryption of Control Signals |
| | Data Link Disruption | -Multiple Data Connection, -Data Connection Encryption |
| | EMI | -Using Special Coatings in UAVs Electronic Systems |
| | Dos/DDoS | -Firewall, -IPS-IDS, -Using High Bandwidth |

Phishing: Attackers can mislead drone users about an important and urgent matter, such as UAV software updates, via fake emails or SMS messages. These messages may contain a bogus update or a bogus security alert and may redirect users to a bogus website or app. This fake website or application can be designed with an interface similar to a real UAV software and may request the user's credentials and access information to gain access to the UAV.

Zero Day Attacks: It can be accomplished by exploiting a vulnerability in the UAV's operating system or software. Using this vulnerability, attackers can attack to control, manage or capture user data.

**Table 5.** Cyber Security Measure for UAV (Other)

| Types | Cyber Attack | Cyber Security Measure |
|---|---|---|
| Other | Phishing | -Awareness Training for Personnel, -Multi-Factor Authentication, -Fake URL Detection Systems, -Spam Filtering |
| | Zero Day Attacks | -Keeping Systems and Software Up-to-Date -Developing Software in Compliance with Secure Software Development Standards |

## 3. Physical Security of Unmanned Aerial Vehicles

### *3.1. Electronic Warfare in Unmanned Aerial Vehicles*

At all stages of a war, electromagnetic spectrum control may have a significant impact on the outcome of military operations. EH is a force multiplier in military operations. EH functions at several levels of conflict, from self-defense to tactical assault strategies. When EH activities are appropriately integrated with other military actions, a considerable effect is obtained. Modern high-tech warfare increasingly emphasizes the use of electronic warfare. Future battlefields will be complex, multilayered, and electromagnetic, and electronic warfare will play a significant role in how the conflict plays out [11].

The UAV is a perfect platform for carrying out numerous electronic warfare tasks due to its fast growth. Unmanned UAV systems can play a unique role in warfare and surveillance in a challenging and dangerous battlefield airspace. EH is the utilization of the electromagnetic spectrum to maximize friendly forces' use of it while preventing an opponent from using it. The overall goal of these technologies, which is the control of the electromagnetic spectrum, may also be described as a military operation. Electronic assault, electronic defence, and electronic assistance make up its three components [12]. Electronic attack (EA): EA is the use of EMS to target people, places, or things in order to weaken, neutralize, or eliminate the capabilities of an adversary [13]. EA can be either passive or active. Jamming, deceit, active cancellation, and electromagnetic pulse (EMP) are all employed in active EA. On the other side, passive EA makes use of stealth, radar reflectors, and traps [14]. In EA, both hard-kill and soft-kill elements are significant. In contrast to anti-radiation missiles, which are designed to damage or destroy radar antennae and equipment, jamming and deception are regarded as soft-kill tactics. Anti- radiation missiles are automatically regarded as hard-kill situations.

Electronic Protection (EP): EP is a subset of EH that consists of both passive and active methods for shielding people, property, and tools from the impacts of friendly or enemy EW use that lowers, neutralizes, or even completely eliminates friendly combat capability [15].

Electronic Support (ES) is a subset of EH that seeks for, intercepts, locates, and/or localizes purposefully and inadvertently emitted EM energy sources in order to recognize threats, focus on them, and prepare for emergencies. Information from ES is used to make judgments on EH operations and other tactical activities including target avoidance, threat avoidance, and target discovery. Information from other intelligence sources is supplemented with information from ES, which offers information in close to real- time. As the name implies, ES offers the data required for operational and planning reasons in EH [16]. Fundamental Electronic Warfare Activities: To put it simply, the basic goal of EH is to take advantage of any openings or vulnerabilities posed by the electromagnetic energy's physics [17], [18].

**Table 6.** List of EW Activities

| | |
|---|---|
| EM Compatibility | Electronic Warfare Reprogramming |
| EM Deception | Emission Control |
| EM Hardening | Spectrum Management |
| EM Interference | Electronic Probing |
| EM Intrusion | Electronic Reconnaissance |
| EM Jamming | Electronic Intelligence |

### *3.2. Hardware Security of Unmanned Aerial Vehicles*

Although UAVs are used in military and civilian applications due to their various advantages, in some cases they are vulnerable to attacks because there is no pilot to control them. This complicates the design of safe and reliable UAVs in order not to cause any harm to themselves or the people around them. When a system is hacked, it can go offline, in which case it is quite difficult to bring the system online. It is insufficient to protect the system using existing information security methods such as encryption or intrusion detection [19]. The threats brought by counter-UAV systems should be known, and precautions should be taken against them. Counter-UAV systems are used as a term covering all UAV physical detection, identification, and tracking systems and neutralization/capture and destruction systems [20]. Counter-UAV systems can be classified as Radar, Acoustic Detection, Kinetic Energy Systems (Ammunition), Collider and Interceptor UAV [21], [22].

Radar: Since military radars are optimized to detect larger and faster aircraft flying high, they cannot be effective in detecting UAVs. UAVs are like birds in that they fly at low speeds and low altitudes. This makes it difficult for radars to distinguish between the two. However, different algorithms and databases are created to distinguish UAVs [20]. UAVs can be made of materials with low radar reflectivity or fly below 100 ft, preventing them from being detected by radar. [23].

Acoustic Detection: Acoustics works with the logic of listening to the sound of the engines and propellers of the UAVs through advanced sound-detection sensors and comparing them with pre-recorded sounds. One of the advantages of acoustic sensing is that by creating a network of sensing devices around the protected area, cost-effective and full global sensing coverage is provided. [20], [23]. Disadvantages of this system: The sound signature of the UAV can be changed, it has low reliability for reliable detection at distances greater than 500 m and is ineffective in residential areas where ambient noise is high. [23], [24]. It can also be imitated by playing an audio recording of a UAV [22].

Kinetic Energy Systems (Ammunition): UAVs are generally weak against kinetic energy ammunition such as guided missiles, smart and air defense munitions, lasers, and firearms. [23], [25]. With kinetic energy systems, UAVs can be dropped with conventional or specially designed ammunition. However, detailed ballistics calculations are required. In the trials, it has been observed that the probability of hitting small UAVs with the ammunition fired from the existing weapons in the inventory is less than 0.7 percent. Besides, using a system with kinetic energy to defend a target in an urban environment can cause collateral damage [26]. Despite these, UAVs must be resistant to this threat and have the ability to escape.

Collider and Interceptor UAV: The colliding UAV application is based on the idea of another UAV hitting the target UAV. However, it is still under development. It is possible to cause unexpected damages when used in residential areas [21]. Although it is not yet considered an advanced technology, it is also aimed at clearly capturing UAVs with interceptive UAVs noise [23], [26].

**Figure 3.** Interceptor UAV [26].

**Figure 4.** Interceptor UAV Catching An Intruder UAV With A Mesh [26].

## 4. Social and Cultural Security of Unmanned Aerial Vehicles

UAVs, which are used semi-autonomously in civil or military industries, require certificates or licenses for operators in most countries. This implies that UAV operators are competent and professional as this field is subject to state authority. However, there is still a possibility of faults or negligence in UAV pilots leading to accidents, which raises doubts in terms of both quality and quantity among authorities responsible for controlling them. While the number of UAVs is increasing rapidly worldwide, control mechanisms are not keeping pace. Although aviation investigations are highly professional, detecting and controlling such a large number of small

aircraft is challenging. Therefore, various software constraints are implemented, but these can be overcome. Drones are used in a wide range of sectors, and the existence of more than one authority can cause issues since they have different purposes of use and can create different problems.

The literature suggests that drones can pose serious concerns regarding the privacy of private life [27]. Therefore, it is recommended to regulate drones to prevent collateral damage. Operators should be trained not only in professional and technical aspects but also in ethical issues to minimize possible negative effects. The use of drones, particularly in military operations, may cause more severe problems regarding international society and international law. Therefore, building a collective legal ground is crucial to prevent this [28].

## 5. Conclusions

According to the findings of this study, Unmanned Aerial Vehicles (UAVs) hold significant promise across a spectrum of applications, spanning both military and civilian domains. The study emphasizes the pivotal role of safety in ensuring the success of UAVs in these diverse applications. Beyond their technical capabilities, the research underscores the importance of a comprehensive security approach, encompassing physical, software, cyber, and social dimensions, to safeguard UAVs from an array of potential threats. Moreover, the study underscores the critical role of public approval in facilitating the widespread integration of UAVs into society. Recognizing and addressing public concerns, particularly regarding security and privacy, emerges as a key factor in gaining the necessary acceptance for these unmanned vehicles. It is asserted that a strategic focus on safety measures, coupled with a responsive approach to public concerns, is essential for UAVs to fully realize their potential, make substantial contributions across various fields, and enhance overall safety and efficiency.

The current state of Unmanned Aerial Vehicles (UAVs) reveals a reliance on human involvement, operating as semi-autonomous systems rather than achieving complete autonomy. Notably, in the civil industry, including applications in agriculture, cartography, and photography, UAVs operate under established aviation rules. However, the military application of UAVs lacks a comprehensive regulatory framework, presenting challenges in addressing issues like collateral damage resulting from operator errors, divergent decision-making assumptions, or intelligence inadequacies. The potential for varied international responses to military UAV operations raises concerns, making it imperative to consider not only the physical, hardware, and cyber security aspects but also the social dimensions of UAV usage. The absence of a universally accepted regulatory model in this realm underscores the need for future international laws to guide the responsible use of UAVs in military contexts. The looming issue of privacy intrusion due to UAV capabilities adds another layer of complexity. While ensuring citizen safety is paramount, authorities must navigate the delicate balance between safeguarding the public and avoiding undue restrictions on individual freedoms. Public opposition to UAV deployment may further complicate matters, potentially hindering technological progress. A notable gap exists in practical experience with fully autonomous UAVs in military operations, highlighting the need for careful consideration and ethical evaluation as technology advances. In essence, the evolving landscape of UAVs demands a comprehensive approach that incorporates legal, ethical, and societal dimensions to ensure responsible and beneficial integration into various industries, particularly in the realm of military applications.

Achieving optimal performance for Unmanned Aerial Vehicles (UAVs) necessitates a cohesive integration of cyber security measures, electronic warfare elements, and hardware features. By designing these components in conjunction with each other, a symbiotic relationship emerges, enhancing both the security of the UAVs themselves and the areas in which they operate. This proactive approach is predicted to fortify the overall security posture of UAVs, addressing vulnerabilities and potential threats across multiple fronts. The interplay between cyber security factors, electronic warfare elements, and hardware features is crucial in creating a resilient and adaptive system. Cyber security measures ensure the protection of digital systems, guarding against unauthorized access and potential cyber threats. Electronic warfare elements contribute to the ability to navigate and operate in contested environments, countering electronic threats effectively. Simultaneously, robust hardware features provide a foundation for reliable and efficient UAV performance. This integrated approach not only safeguards the UAVs from potential cyber-attacks but also fortifies their operational domains, mitigating risks and enhancing the overall effectiveness of their missions. As technology continues to advance, this predictive strategy underscores the importance of a holistic and multidimensional security framework to meet the evolving challenges faced by UAVs in the modern landscape.

## References


[1] Albeaino, G., Gheisari, M., & Franz, B. A. (2019). A systematic review of unmanned aerial vehicle application areas and technologies in the AEC domain. Journal of Information Technology in Construction, 24(20), 381–405. https://www.itcon.org/papers/2019_20-ITcon-Albeaino.pdf

[2] Afghah, F., Razi, A., Chakareski, J., & Ashdown, J. (2019). Wildfire Monitoring in Remote Areas using Autonomous Unmanned Aerial Vehicles. Conference on Computer Communications Workshops. https://doi.org/10.1109/infcomw.2019.8845309

[3] Laghari, A. A., Jumani, A. K., Laghari, R. A., & Nawaz, H. (2022). Unmanned aerial vehicles: A review. Cognitive Robotics, 3, 8–22. https://doi.org/10.1016/j.cogr.2022.12.004

[4] Hartmann, K., & Giles, K. (2016b). UAV exploitation: A new domain for cyber power. International Conference on Cyber Conflict. https://doi.org/10.1109/cycon.2016.7529436

[5] Shepard, D. P., Bhatti, J. A., Humphreys, T. E., & Fansler, A. A. (2012b). Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks. Proceedings of the 25th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2012), 3591–3605. https://doi.org/10.15781/t2xw48c62

[6] Krishna, C. G. L., & Murphy, R. R. (2017). A review on cybersecurity vulnerabilities for unmanned aerial vehicles. International Symposium on Safety, Security, and Rescue Robotics. https://doi.org/10.1109/ssrr.2017.8088163

[7] Fourati, L. C., Chahbani, S., & Rezgui, J. (2020). Vulnerabilities Assessment for Unmanned Aerial Vehicles Communication Systems. International Symposium on Networks, Computers and Communications. https://doi.org/10.1109/isncc49221.2020.9297293

[8] Shane, S., & Sanger, D. E. (2011). Drone crash in Iran reveals secret US surveillance effort. The New York Times, 7.

[9] Kim, A. W., Wampler, B. L., Goppert, J., Hwang, I., & Aldridge, H. (2012). Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles. Infotech@Aerospace 2012. https://doi.org/10.2514/6.2012- 2438

[10] Dahiya, S., & Garg, M. (2019). Unmanned Aerial Vehicles: Vulnerability to Cyber Attacks. Springer EBooks, 201–211. https://doi.org/10.1007/978-3-030-37393-1_18

[11] Sharma, P., Sarma, K. K., & Mastorakis, N. E. (2020). Artificial intelligence aided electronic warfare systems-recent trends and evolving applications. IEEE Access, 8, 224761-224780.

[12] Tkachenko, O. Y. (2015, October). System of electronic warfare with uavs. In 2015 IEEE International Conference Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD) (pp. 324-327). IEEE.

[13] Lei, L., Gao, Y., Wang, X., Zhang, P., & Guo, S. (2009). Design and Realization of Virtual Scene System in UAV Electronic Warfare. In 2009 International Conference on Information Engineering and Computer Science (pp. 1-4). IEEE.

[14] Spezio, A. E. (2002). Electronic warfare systems. IEEE Transactions on Microwave Theory and Techniques, 50(3), 633-644.

[15] Bommakanti, K. (2019). Soft Kill'or 'Hard Kill'? The Requirements for India's Space and Counter-Space Capabilities. ORF Occasional Paper, (224).

[16] Mei, H., & Bo, X. (2022, November). A Real time Decision Making Method of Electronic Warfare Based on the Protection of Key Points. In 2022 6th International Symposium on Computer Science and Intelligent Control (ISCSIC) (pp. 195-199). IEEE.

[17] Kuzdeba, S., Radlbeck, A., & Anderson, M. (2018, October). Performance metrics for cognitive electronic warfare-electronic support measures. In MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM) (pp. 1-9). IEEE.

[18] Lazarov, L. (2019, March). Perspectives and trends for the development of electronic warfare systems. In 2019 International Conference on Creative Business for Smart and Sustainable Growth (CREBUS) (pp. 1- 3). IEEE.

[19] Rani C, Modares H, Sriram R, Mikulski D, Lewis FL. Security of unmanned aerial vehicle systems against cyber-physical attacks. The Journal of Defense Modeling and Simulation. 13(3):331-342, 2016. doi:10.1177/1548512915617252.

[20] Tiurin V, Mirnenko V, Openko P. General approach to counter unmanned aerial vehicles. Safety & Defense, 5, 6-12, 2016.

[21] Yusuf, G. E. N. Ç., & Erciyes, E. İnsansız hava araçları (İHA) tehditleri ve güvenlik yönetimi. Türkiye insansız hava araçları dergisi, 2(2), 36- 42, 2020.

[22] Sathyamoorthy, D. A Review Of Security Threats Of Unmanned Aerial Vehicles And Mitigation Steps The Journal of Defence and Security; Kuala Lumpur Vol. 6, Iss. 1, 2015.

[23] Humpreys, T., Statement on the Security Threat Posed by Unmanned Aerial Systems and Possible Countermeasures. Statement to the Subcommittee on Oversight and Management Efficiency of the House Committee on Homeland Security, Washington D.C., 2015.

[24] Naboulsi, Z., Drone Detection: What Works and What Doesn't. Available online at: http://www.net-security.org/article.php?id=2297 (Last access date: 09 April 2023).

[25] Chuter, A., Mini drones spark heightened interest in countering threat. Defense News, 22 June 2015.

[26] Gayle, D., The Drone Catcher: Flying Net Is Designed to Stop Terrorists from Flying Bomb-Laden Gadgets Into Nuclear Power Stations. Available online at: http://www.dailymail.co.uk/news/article- 2948062/The-drone-catcher-France-reveals-flying-netstop-terrorists- flying-bomb-laden-gadgets-nuclear-power-stations-following-spate-sightings.html (Last access date: 09 April 2023).

[27] Gettinger, D., Domestic Drone Threats. Available online at: http://dronecenter.bard.edu/whatyou-need-to-know-about-domestic- drone-threats (Last access date: 09 April 2023).

[28] Wilson, R. L. (2014, May). Ethical issues with use of drone aircraft. In 2014 IEEE International Symposium on Ethics in Science, Technology and Engineering (pp. 1-4). IEEE.